(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 439 495 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
21.07.2004 Bulletin 2004/30

(51) Int Cl.[7]: **G07B 15/00**, G07C 9/00

(21) Application number: **03001026.8**

(22) Date of filing: **17.01.2003**

(84) Designated Contracting States:
AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HU IE IT LI LU MC NL PT SE SI SK TR
Designated Extension States:
AL LT LV MK RO

(71) Applicant: **SIEMENS AKTIENGESELLSCHAFT**
80333 München (DE)

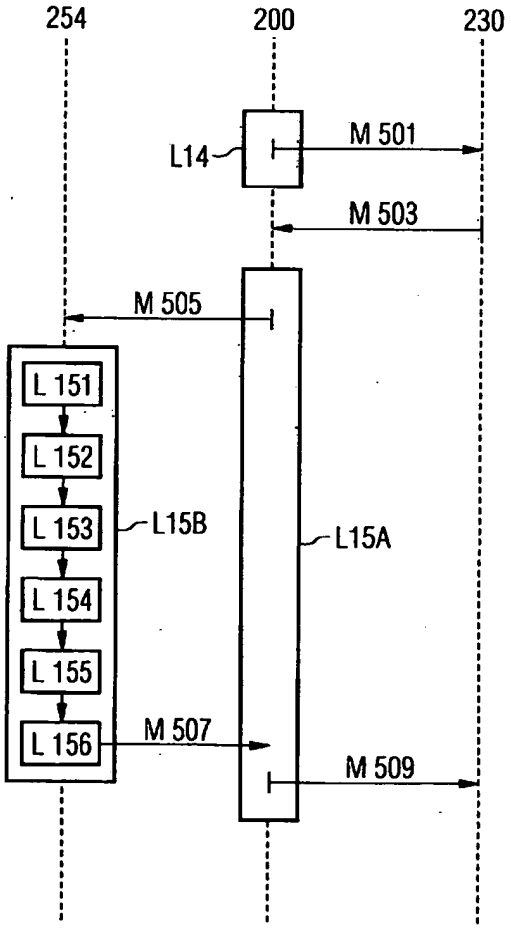
(72) Inventor: **Roldan, Carmen Santa Cruz**
DK-9000 Aalborg (DK)

Remarks:
Amended claims in accordance with Rule 86 (2) EPC.

(54) Electronic ticket, system and method for issuing electronic tickets, and devices and methods for using and performing operations on electronic tickets

(57) A system for validating an electronic ticket includes i) receiving means (263) for receiving an electronic ticket, the electronic ticket including a first identifier (TUID1) and a second identifier (NONCE'), ii) a ticket storage (230) for storing the electronic ticket, iii) secure storing means (252) for storing the first identifier (TUID), and iv) validating means (280) adapted to store the first identifier (TUID) to the secure storing means (252) when the electronic ticket is validated. An electronic ticket (300) has a sealed state and a validated state, wherein the state of the electronic ticket (300) is defined by the public part (300PU) or private part (300PR) of the electronic ticket (300), in such a manner that whenever the private part (300PR) corresponds to a valid value, the electronic ticket (300) is in the validated state.

FIG 5



EP 1 439 495 A1

Description

Field of the Invention

[0001] The invention relates generally to electronic tickets or documents, and, more specifically, to generating, transferring, and presenting such tickets or documents.

Background of the Invention

[0002] Digital or electronic tickets have been under a growing interest among the general public. Therefore, various players in the industry have designed different approaches which are to enable a flexible and fast usage of tickets without any compromising of the security.

[0003] Because of the obvious advantages obtained by using a standardised methodology, the development work has lead to the establishment of several standardisation bodies. An example of such a standardisation body is the Mobile electronic Transactions MeT. The MeT concentrates on various aspects relating to electronic transactions and currently (January 7, 2003) has a website www.mobiletransaction.org.

[0004] The technology used for the administration and usage of tickets needs to be defined in order for electronic tickets to reach a commercial success. The MeT has so far published a Discussion Document MeT Ticketing Framework, Version 1.0 (February 21, 2001) which at the moment may (January 7, 2003) be downloaded from http://www.mobiletransaction.org/pdf/R11/MeT-Ticketing-Framework-R11.pdf.

[0005] Several other documents, such as Coupon ticketing, Version B (November 20, 2001), at the time of writing available at http://www.mobiletransaction.org/pdf/R11/MeT-Coupon Ticketing-R11.pdf, and MeT Ticketing Wallet Server, Version B, (July 09, 2001), at the time of writing available at http://www.mobiletransaction.org/pdf/R11/MeT-Ticketing Wallet-Server-R11.pdf), have also been presented.

[0006] Figure 1A illustrates a system in which electronic tickets may be used. A ticket is issued by a ticket issuing system 101 which is connected to a communications network, such as the Internet 100B usually via its front end 1011. Most ticket issuing systems 101 include also a back end 1012 which performs the ticketing and stores a copy of issued tickets to a data storage 1013. When a ticket has been generated in the ticket issuing system 101, it is usually sent to a personal computer 104 via the Internet 100B, or to some mobile device 102 or 103 which may be connected to the Internet 100B either directly through a PC or via a mobile network 100A, such as a GSM, GPRS, or UMTS network.

[0007] Tickets may be ordered directly from the personal computer 104, or from the mobile devices 102, 103. Some ticket models are push-type, wherein the ticket issuing system pushes the ticket to the device of the end-user, whereas some ticket models are pull-type which involve a request from the end-user device before the ticket is generated. Further, a ticket may be ordered by a first mobile device 102 and used by the user of a second mobile device 103.

[0008] Further, usually the system contains an inspection system 106 which is intented to check the tickets. After checking the tickets a person presenting the ticket is allowed a service, such as entering an airplane or through a gate. Because electronic tickets can be used within a communications network, such as the Internet 100B, also for paying services available in, from, or via the network, the nature of the inspection system 106 is not limited to these but may involve also other tasks.

[0009] In some cases the system also includes a ticket printer 105. This kind of approach has proved to be particularly valuable when the service provider in question is willing to enable the use of traditional tickets as well. The conventional paper-form tickets are fast to check by a human inspector. Thus it may be beneficiary to print a paper ticket of an electronic ticket with which the user is then allowed the service. Therefore the ticket printer 105 which may also be connected to the Internet 100B obtains instructions from the ticket issuing system 101 relating to what kinds of tickets to accept. Ticket printer 105 may include similar functionalities to the inspection system 106.

[0010] Evidently, there is not yet any agreement about the future format of an electronic ticket. The solutions used by current vendors and already being available in the market seem not to be satisfactory in all aspects. Thus there still exists a need for a flexible and general ticket concept which provides the ticket issuers and users of the tickets with a high enough security level, and which is technically efficient to use whatever the final form of the electronic appearance of the electronic ticket will be.

[0011] Especially the issuing of an electronic ticket has preferably to be fast, reliable and it should not consume too much air interface nor introduce too much disturbances into the air interface. An essential issue related to the issuing of such electronic tickets is that they need be validated. Problematic, in both technical and therefore also in economical terms, has turned out to be the structure of those means, preferably in the user device, which should take care of performing the validating procedure, for cardboard tickets is also known as stamping.

[0012] All prior solutions except one proposed by Siemens require that there is an on-line connection between the ticket issuer and the secure element in the mobile device of the ticket user. The main reason for this is to establish an

immediate link (or validation) between the secure element and the ticket, with a procedure that starts prior ticket delivery and usually concludes once the ticket is received in the device. On one hand, this kind of approach is very rigid because it relies on the availability of the secure element during the whole process of ticket request and delivery. Consequently, if the secure element is not available at a given moment of this process, the ticket will become useless since the validation of the ticket would not be completed. On the other hand, if the tickets are explictly and permantely linked to a given secure element after validation, then it remains a problem how the ticket can be transferred to be used in another device with another secure element (e.g. by another user). Finally, the on-line access to the secure element during the ticket request and delivery prohibits the possibility of asynchronous delivery modes, such as the Multimedia Messaging Service MMS, or using different delivery means, especially the Internet.

[0013] The contribution by Siemens suggested that a real-time clock could be used to achieve delayed validation. This, however, has turned out to be technologically too complicated, as a secure real time clock located in the user device is at the moment too expensive to construct. So, it still remains as a problem how to delayed the validation of a given ticket with the secure element while keeping a high security level of copy protection of the ticket.

[0014] It is an object of the invention to bring about a solution by means of which it is possible to obtain a reliable, efficient and flexible ticketing platform, electronic ticket, and/or device for using electronic tickets, and/or device for inspecting electronic tickets, in such a manner that the ticket validation, when high level of copy protection is required, can be implemented without too complex and difficult mechanism. Another objects are to provide solutions by means of which it is possible to transfer electronic tickets. Still another object of the invention is to bring about a novel electronic ticket model.

Summary of the Invention

[0015] This and other objectives of the invention can be achieved with a method and a system according to any one of the independent patent claims.

[0016] A device for validating an electronic ticket includes i) receiving means for receiving an electronic ticket, the electronic ticket including a first identifier and a second identifier, ii) a ticket storage for storing the electronic ticket, iii) secure storing means for storing the first identifier, and iv) validating means adapted to store the first identifier to the secure storing means when the electronic ticket is validated. By using such a device a non-real-time validation of electronic tickets is enabled without an expensive and technically complicated real time clock. Further, during the validation procedure no continuous connection between the ticket issuing system and the device is needed.

[0017] According to one aspect of the present invention, the device for validating an electronic ticket may further include security means for verifying the origin of the electronic ticket, preferably by decrypting at least a part of ticket containing said first and second identifiers, especially using a private key assigned to a trusted agent. Such an arrangement brings about an enhanced security. The issuer can now be authenticed, which makes the ticket application and ticket application system more harder to crack by malicious parties.

[0018] According to one further aspect of the present invention, a device for presenting an electronic ticket includes presenting means for presenting the first identifier and the second identifier in order to use said electronic ticket. In such a manner the electronic ticket can be presented in a convenient manner, and copy protection can also be obtained. When the ticket application and/or security means are safe, then it can also be ensured that the electronic ticket cannot be presented multiple times if that is not allowed.

[0019] According to a further aspect of the present invention the device for presenting an electronic ticket can further include means for verifying the identity of an entity to which the electronic ticket is going to be presented. Such an arrangement brings about an enhanced security. The ticket inspetion system or ticket printer can now be authenticed, which makes the ticket application and ticket application system more harder to crack by malicious parties.

[0020] According to a further aspect of the present invention, a device for validating and/or presenting an electronic ticket can further include i) generation means adapted to generate at least one third identifier; and whereby the secure storing means are adapted to store the third identifier and/or the ticket storage is adapted to store the third identifier. Such an arrangement enables the use of multi-use tickets and serial tickets.

[0021] A device for validating and/or presenting an electronic ticket can further include i) generation means adapted to generate a second identifier, ii) generation means adapted to generate a ticket issuing request including the second identifier generated and iii) sending means for sending the ticket issuing request to a ticket issuing system. If a request is generated in this manner, based on the identifier, the ticket issuing system can ensure that the electronic tickets oredered really are what the user or the device has been subscribing.

[0022] A device for validating and/or presenting an electronic ticket can further includes means for changing the third identifier in the ticket storage and/or in the secure storing means in response to a change request, especially relating to said using or transfer of the electronic ticket, or in response to using the ticket, such as received from an entity to which the electronic ticket is presented. In such a manner serial tickets can be shared between users, one user can transfer his/her tickets to another user, and a user can ask another user to subscribe a copy-protected ticket on behalf

of him/herself.

[0023] A ticket issuing system or a device for issuing an electronic ticket includes includes generation means adapted to generate an electronic ticket responsive to a request including a first identifier and a second identifier, especially when the request has been generated by a device for validating an electronic ticket, and where the ticket includes a first identifier or an identifier derived therefrom. Such a ticket issuing system or device enables the operation of a ticket validation device, and by using such a system or device a delayed validation of copy-protected tickets can be obtained.

[0024] A ticket issuing system or a device for issuing an electronic ticket can further include means for sealing the electronic ticket. This enhances the security of the electronic ticket, because the issuer can now ensure that only a trusted user is able to validate the ticket.

[0025] A device for requesting the use of an electronic ticket includes generation means for generating a request for using an electronic ticket, the request including a refresh value for a second identifier of an electronic ticket. Such a device enables the use of copy-protected electronic tickets that have been validated not in real-time.

[0026] A device for requesting the use of an electronic ticket may further include broadcasting means for broadcasting a product tag or other identifier describing ticket types supported by the device. So the ticket application can be advised to select only such tickets that are currently usable. In this manner, costly and extremely difficult implementation of recovery mechanisms for invalidly used tickets can be avoided.

[0027] A mobile device may further include receiving means for the user to select which ticket to be presented, especially if there are more than one ticket in the ticket storage. In this manner the system can be made more user-friendlier because the user can ge given the freedom of choice while still retaining the certainty that only valid tickets are going to be presented and so saving the difficult implementation of recovery mechanisms.

[0028] An electronic ticket has a sealed state and a validated state, wherein the state of the electronic ticket is defined by the public part or private part of the electronic ticket, in such a manner that whenever the private part corresponds to a valid value, the ticket is in the validated state. Such an electronic ticket enables the delayed validation for a copy protected ticket.

[0029] The valid value for private part corresponds to an identifier stored in security means of a mobile device. In this way also the ticket inspection system or the ticket issuing system can make sure that it is only a trusted client that is going to validate and/or to use the electronic ticket.

Brief description of the drawings

[0030] In the following, the invention and its preferred embodiments are described more closely referring to the examples shown in Figures 1B to 7 in the appended drawings, wherein:

Figure 1A	illustrates a system for providing and using electronic tickets;
Figure 1B	is a schematic block diagram of inspection system 106;
Figure 1C	shows a user with a mobile device 102 approaching the inspection system 106;
Figure 2A	is a block diagram of a mobile device 102 adapted to carry out the present invention;
Figure 2B	shows contents of registry 722 before a registration;
Figure 2C	shows contents of a registry 722 after a registration;
Figures 3A, 3B, and 3C	illustrate a preferable format for the electronic ticket 300;
Figure 4	shows a preferred embodiment of a process for issuing a ticket;
Figure 5	shows a preferred embodiment of a process for validating a ticket;
Figures 6A and 6B	show a preferred embodiment for a process for using a ticket; and
Figure 7	shows a preferred embodiment for process of splitting and transferring a ticket.

[0031] Like reference signs refer to corresponding parts and elements throughout Figures 1-7.

Detailed description of the invention

[0032] Figure 1B is a block diagram of an inspection system 106. Its operation is described below in more detail together with some further aspects of the present invention. The inspection system 106 includes transport means 805, proximity detection means 802, proximity discrimination means 803, storage 807, and ticketing means 814.

[0033] As the reader may know, proximity detection means 802 are usually based on optical or magnetic sensors that detect which device is the closest in any given moment. As an alternative, proximity discrimination means 803 can correspond to detecting a new BLUETOOTH address, or comparing an addresses detected with at least one predetermined address, for example.

[0034] The transport means 805 include point to point sending means 804 for sending user-specific messages, broadcasting means 801, and receiving means 806. The ticketing means 814 include generation means 808, comparison means 809, verification means 810, and parsing means 811; the main purpose of the ticketing means 814 is to broadcast product tag 721 supported by the inspection system 106, to generate user-specific ticket presentation requests, and to verify the integrity and origin of the tickets presented by any mobile device 102, 103.

[0035] Broadcasting means 801 act in the proximity of the inspection system 106, and transport messages including the value of a product tag 721 of a given ticket class. The product tag 721, as will be explained below, identifies the required ticket to be presented to the inspection system 106 in order to access a given service.

[0036] Receiving means 806 are used to receive ticket elements related to the ticket use.

[0037] Generation means 808 are used to generate new nonces 704. Parsing means 811 are used for extracting a nonce 704 of the private part 300PR in ticket data 706. Comparison means 809 are used to compare the nonce 704 of the ticket with the nonces stored in the storage 807. Verification means 810 are used to verify that the ticket data object 303 has not been tampered with, and for comparing the trusted agent signature 709 with the ticket data 706.

[0038] Some purposes of the proximity detection means 802 are: i) to discover the users that are within a given distance range of the inspection system 106, ii) to discriminate among such users either by detecting the closest one, or on the basis of their individual device addresses, and iii) that only users sufficiently close to the inspection system 106 are presented with an individual ticket presentation request REQ4 containing a product tag 721 and a unique nonce 704. The ticket presentation request REQ4 is presented to the mobile device 102 by using any suitable point-to-point sending means 804 available.

[0039] Storage 807 is used for employed to storing the generated nonce values that later are compared with those transported on an electronic ticket 300.

[0040] Figure 1C shows a user with a mobile device 102 approaching the inspection system 106. The proximity range ΔR_1 of the proximity detection means 802 corresponding to current technology is about 10 m if the proximity detection means include a transmitter with 4 W power and the mobile device 102 includes a passive component, such as an RF tag. Of course any other proximity detection method can be used instead or in combination with an RF tag. The proximity range may be adapted to show non-uniform directional characteristics, say that $\Delta R_1 << \Delta R_2$ in order to ensure proper functioning, for example in the vicinity of a gate at the airport. In order to obtain these non-uniform directional characteristics, proper shielding means 199 can be used. Such shielding means 199 can be simply opaque plastics or metal (aluminum, steel, lead), depending on the broadcasting means 801. If the broadcasting means 801 include communication by using visible or infra-red light, then shielding can be obtained by selecting a proper distribution of opaque and transparent material around the broadcasting means 801. For RF signals, however, a heavier shielding is necessary.

[0041] The inspection system 106 broadcasts product tag 721 which is then detected by the mobile device 102. This is discussed in more detail below together with Figures 6A and 6B.

[0042] Figure 2A is a block diagram of a mobile device 102. In principle, the mobile device 102 can be any portable device, such as a Personal Digital Assistant PDA, a laptop computer, a Portable Digital Wallet, or a Personal Trusted Device PTD.

[0043] In the following it is for simplicity assumed that the mobile device 102 is a mobile terminal, such as a mobile phone, having capabilities to be in connection via remote transportation means such as the mobile network 100A and the Internet 100B, as well as via local transportation means such as BLUETOOTH and IrDA, with the ticket issuing system 101 and with the ticket inspection system 106.

[0044] The mobile device 102 includes input/output I/O means 260 which include receiving means 263, sending means 262, and a display 261. The receiving means 263 include means with which the mobile device 102 can receive any data from a mobile network 100A, from another mobile device 103, from the user of the mobile device 102, from inspection system 106, ticket issuing system 101, and so on. The receiving means 263 can comprise a keyboard, wireless communication means, touch screen, joystick, speech recognition system adapted to work with a microphone, and so on.

[0045] Further, the mobile device 102 may also include a loudspeaker 264 and a Radio Frequency RF tag 265. The RF tag is usually a contactless smart card. On the market there are also some models known as hybrid smart cards

comprising both an electrical interface, preferably to the SIM card, and an RF interface.

[0046] The mobile device 102 includes also security means 250. The security means 250 include simple ticket security means 224 for providing simple ticket security services, such as simple copy protection, preferably by (a) own ticket application 200 implemetantion and/or (b) by the usage of weak symmetric encryption by any given algorithm.

[0047] The security means 250 can further include means for providing high-level security services to the mobile device. These means can include a specific tamper-proof (or tamper-resistant) security component called security element security element 252 corresponding to secure storing means.

[0048] The security element 252 is preferably located inside the mobile device 102, and either integrated into it, or provided as a detachable part.

[0049] The high-level security services provided by the security element 252 to the mobile device 102, includes means for generation of random numbers, strong symmetric cryptography, and Public Key Infrastructure PKI cryptography. Regarding PKI, the security element 252 can also provide other services related to it, such as handling of certificates (e.g root certificate storage, certificate path discovering and validation), storing of key pairs, digitally signing documents, and authentising of digital signatures. When the mobile device 102 is a mobile phone and the security means 250 further comprise a security element 252 such as the one described above, the mobile phone is then called a personal trusted device or PTD.

[0050] A current example of a security element 252 adjusted to the prior definition is a Wireless Identity Module WIM defined in the Wireless Application Protocol WAP standard. The WIM provides cryptographic services, such as PKI encryption, and handling and generation of digital signatures for different mobile based applications.

[0051] The security element 252 may further include a trusted agent 254 whose purpose is to provide specific copy protection services involving the use of strong cryptography to different applications, and in particular the ticket application 200, and thus interact through the latter with the ticket issuing system 101, inspection system 106 and, further, even with a ticket application system 723' of a second mobile device 103.

[0052] The copy protection services provided by the trusted agent 254 may involve the use of PKI cryptography. In this case, the trusted agent 254 uses one or more dedicated key pairs which are initially solely employed for copy protection services. In addition, the trusted agent 254 has an access to a registry 722, preferably inside the security element 252.

[0053] A ticket application system 723 comprises ticket application 200 preferably stored in the mobile device 102, simple ticket security means 224, trusted agent 254 (preferably stored in a security element 252), and dedicated registry 722 preferably stored in a security element 252. The structure and use of the registry 722 is explained in more detail with Figures 2B and 2C.

[0054] In the following description of the preferred embodiment of ticket application system 723 it is assumed that the security element 252 is a smart card offering PKI services to the ticket application 200 through the trusted agent 254 and that by using such services the ticket application 200 achieves a high-level ticket security.

[0055] An electronic ticket 300 received from the ticket issuing system 101 is stored into ticket storage 230 which may be a database or memory including a register. The ticket storage 230 includes tickets 729 and serves them to the ticket application 200. The ticket storage 230 includes also processed nonces 730 generated by the trusted agent 254.

[0056] The User Interface U/I part 201 of the ticket application 200 performs various functions. Firstly, with the help of the U/I part 201 the user may subscribe tickets from the ticket issuing system 101. Secondly, the U/I part 201 notifies the user whenever an electronic ticket 300 is received. The user may then have an opportunity to confirm the storing of an electronic ticket 300 or to reject it. Thirdly, when the user is willing to use the electronic ticket 300, he/she may select it to be presented by selecting it from a menu in the U/I part 201.

[0057] The ticket application 200 which preferably is located in the mobile device 102 further comprises parsing means 202, comparison means 204, generation means 206, and validating means 280.

[0058] When an electronic ticket 300, i.e. any one of the tickets 729 stored in the ticket storage 230, is to be used, the parsing means 202 read the contents of the electronic ticket 300. Because several components of the electronic ticket 300 are implemented using an extensible Markup Language XML frame, the parsing means 202 can be adapted to detect a predefined keyword inside the electronic ticket 300. This predefined keyword is preferably contained within the element PTD information 703. The point of the keyword indicates the presence and location of a referenced ticket data object 303 or the presence of an embedded ticket data object 303 inside the PTD information 703. The parsing means 202 go thus through the parseable part of the ticket and produce a parsing result. This is described in more detail below with Figures 3A to 3C.

[0059] In the comparison means 204 the parsing result is checked. If the parsing result indicates that the keyword was detected, i.e. that the presence and location of the referred ticket object 303 (or that the presence of an embedded ticket object) was found, in the generation means 206 a presenting request is generated. In the opposite case no presenting request will be generated. The selection of the presenting means 260B may be constrained or indicated explicitly by the issuer; then the presenting means 260B are specified preferably within the ticket presentation information 705 by using a predefined identifier which either the ticket application 200 or the presenting means 260B have

been adapted to recognise.

[0060] The presenting request is passed to the presenting means 260B comprising of a plurality of presenting means 260B, such as display 261, sending means 262, loudspeaker 264, and RF tag 265, depending on the ticket type. The presenting means 260B present the ticket object 303. Depending of the presenting means 260B selected, the presenting of the ticket object 303 takes place by displaying it on the display 261 (for a barcode or an image), by playing it through a the loudspeaker 264 thus producing an aurally recognisable tone, by beaconing the ticket object 303 i.e. storing the ticket object 303 as a whole or only an ID refererring to the object into an RF tag 265 which then beacons (such as sends as a Radio Frequency signal) the ticket object 303 when brough close enough to a check point, or in some other suitable way.

[0061] One possibility for presenting the ticket object 303 is to present it using sending means 262. Possibilities for the sending means 262 include normal mobile communication means, i.e. for sending the object via a mobile network communication channel, such as per short message SMS, EMS, or MMS message, or in a data packet. Also other possibilities exist, such as presenting the ticket data object by using a low-power RF chip such as the BLUETOOTH, or by presenting it using infra-red such as IrDA means, and so forth. If some of the mobile network communication channels or BLUETOOTH is to be used, the presentation of the object is then preferably addressed to a predefined address in order for the recipient of the presentation, i.e. the inspection system 106 or the ticket printer 105 or 106 receives the presentation.

[0062] Figures 2B and 2C show contents of registry 722 before and after registration, respectively. In the exemplary registry there are three registers 724A, 724B, and 724C. Each of registers 724A-C include TUID field 725 and nonce field 726.

[0063] As can be seen in Figure 2B, before registration the nonce field 726A of the register 724A includes nonce 727A, the nonce field 726B of the register 724B includes nonce 727B, and so forth, but the TUID fields 725 in all registers 724A-C are empty. The nonces 727A-727B correspond to random numbers which have been generated by the trusted agent 254 responsive to a request M411 from the ticket application 200. After generating the nonces 727A-727C the trusted agent 254 passes them as processed nonces 727A'-727C' to the ticket storage 230 and stores them unprocessed in its own registry 722 into registers 724A-724C and corresponding NONCE fields 726A-726C. This is discussed in more detail with reference to Figure 4 below. The nonces 727A-727B can also be a URI generated by the trusted agent 254, or any other suitable identifier.

[0064] As can be seen in Figure 2C, after registration the different registers 724A-C in the registry 722 include also values in corresponding TUID fields 725A-C, respectively.

[0065] When an electronic ticket 300 having ticket unique identifier 702A has been ordered, the ticket application 200 has sent a processed nonce 727A' to the ticket issuing system 101, in this case processed nonce 727A' is the nonce 727A together with its digital signature. When the ticket issuing system then returns the electronic ticket 300, the message including the ticket includes not only nonce 727A but also ticket unique identifier 702A. When the electronic ticket 300 is then registered, i.e. validated, the value of TUID 702A is stored into TUID field 724A corresponding to nonce field 726.

[0066] In a similar manner, for another electronic ticket 300 which has another TUID 702B and nonce 727B, the validating means that the TUID field 725B in the register 724B of the registry 722 is updated, and so forth. Then the status of the registry shows whether or not there are any nonces available in different registers. It is clear that the number of registers is not limited to three, but depends only on the amount of memory available.

[0067] The nonces can be used by the ticket application 200 to request an electronic ticket 300. Alternatively, a nonce can be passed to another mobile device 103, the another mobile device 103 having a corresponding ticket application 200', for the another mobile device 103 to request an electronic ticket 300 on behalf of the trusted agent 254 of the first mobile device 102.

[0068] When a signed nonce is either used to request a ticket 300, or transferred to another mobile device 103 through any of the available sending means 262 of the mobile device 102, the ticket application 200 marks the particular signed nonce used.

[0069] Figures 3A, 3B, and 3C illustrate a possible structure of an electronic ticket 300 and its different parts. The electronic ticket 300 includes user information 301 and ticket application information 302.

[0070] Figure 3A shows different elements of an electronic ticket 300. User information 301 is information to the user on the services, terms, and conditions of use of the electronic ticket. Ticket application information 302 presents two interfaces, one for each of two of the preferable components of the ticket application system 723, namely; (a) the ticket application 200 preferably stored in the mobile device 102, and (b) the trusted agent 254 that is preferably stored in security element 252, and where the latter might either be an integrated or detachable component to the mobile device 102. Thus, the corresponding interfaces inside the ticket application information 302 are the PTD information 703, and the security element information 701.

[0071] The PTD information 703 further comprises at least some of the following: product tag 721, presentation information 705, security information 707, and ticket object 303.

[0072] Product tag 721 indicates the type of ticket to the ticket application 200. The purpose of this tag is to allow a fast search in the ticket storage 230 for a given ticket product marked with product tag 721. In the case that there are several tickets among the tickets 729 matching the searching criteria, the user will be requested to choose which one should be presented to the inspection system 106.

[0073] Presentation information 705 indicates to the ticket application 200 which presenting means 260B of the mobile device 102 is preferably to be used for presenting the ticket data object 303.

[0074] Security information 707 indicates the security requirements to the ticket application 200 in regard of the ticket data object 303. These requirements need not be performed by the security element 252, and thus can be implemented by the simple ticket security means 224.

[0075] Ticket object 303 is presented by the ticketing applicaton 200 to the inspection system 106 in order to gain access to a given service. Consequently, it is also the object that needs to be protected. To achieve a high level of copy protection, the ticket object 303 has to include a ticket unique identifier TUID 702. Further, the ticket unique identifier 702 should be identical to that stored in the security element information 701.

[0076] With further regards to the ticket object 303, it can be protected against modification of its content by adequate means provided before hand by the issuing system 101. This means can be encryption, issuer signature 708 by using the issuing system PKI signature, and/or complex or even obscure coding. Some of this means can also be used for achieving obfuscation of the ticket object 303.

[0077] A trusted agent 254 can be used to protect the ticket object 303 against illegal duplication and double expending. This provides a high level of security, especially when the trusted agent 254 is located inside the security element 252. The security element information 701 includes information necessary for the trusted agent 254. The security element information 701 can further include any of the following subelements: i) ticket unique identifier 702 , ii) nonce 704, iii) N of uses 711, especially a field value indicating multiple use in case of a multiple use ticket, and/or iv) signature element 731.

[0078] The ticket unique identifier 702 is preferably common to the ticket object 303. Nonce 704 corresponds to a version control identifier. The signature element 731 contains the issuer signature 708' of the security element information 701 (excluding the signature itself) for an electronic ticket 300 in sealed state. When the electronic ticket 300 is registered with the trusted agent and the ticket is in so-called validated state, the signature element contains the trusted agent signature 709 of the security element information 701 (excluding the signature itself).

[0079] Ticket value data 720 is the "ticket value" information within the ticket object 303, and it is necessary for accessing a service offered. It is not the price tag but can nevertheless correspond to monetary information, such as describing the price or value of the electronic ticket 300. This is particularly useful when the value of the service for which the electronic ticket 300 is spent changes or has changed between the issuing of the ticket and the consuming of the service. The user can be requested to pay more, the amount of payment then depending on the price change, or in the opposite case the user can be credited for the price difference.

[0080] In the preferred embodiment of the invention, the ticket object 303 can be in any given format and content as defined by the issuer, the other parts of the electronic ticket 300 are a part of an XML document, except for the security element information 701. This latter information, likewise the ticket object 303 itself, can be referred to or otherwise embedded in the XML document part, such as in the ticket application information 302. Consequently, the security element information 701 can have a format that is more easily handled by current smart card technology.

[0081] In order to achieve a high level of security for the copy protection of the ticket object 303, by the means of the security element information 701, the latter can implicitly be linked to a given trusted agent 254, located in a particular security element 252. Furthermore, both items, ticket object 303 and security element information 701, are preferably presented during ticket use to the inspection system 106.

[0082] In view of the above, the elements of an electronic ticket 300 can be considered to belong to two different classes as shown in Figure 3A, namely to public part 300PU and to private part 300PR. In the public part 300PU, if an authentication of any part of the data is needed, this will be preferably achieved by means of the verification of the issuer signature 708, i.e. a digital signature of the issuing system 101. In the private part 300PR there are two cases; when the electronic ticket 300 is in a sealed state, and when it is in a registered state.

[0083] Figure 3B illustrates some differences between the electronic ticket 300 in a sealed or in a registered state in more detail:

[0084] If the electronic ticket 300 is in the sealed state, the authentication of the corresponding data (i.e. security element information 701) performed by the trusted agent 254 is achieved by means of the verifying the issuer signature 708' of the issuing system 101. If the electronic ticket 300 is in the validated state, the authentication of the correspoing data (i.e. security element information 701) is performed by either the trusted agent 254, or the inspection system 106, and it involves the verification of the trusted agent signature 709.

[0085] The description of the preferred embodiment for the ticketing processes of (1) request, (2) issuing & delivery, (3) registration, (4) use and (5) transfer refers to the security element information 701 as private part 300PR, and to the rest of ticket elements as public part 300PU.

[0086] Figure 3C illustrates the state change of an electronic ticket 300. The state of the electronic ticket 300 is changed from a sealed to a validated state primarily by effecting the change of the 300PR sealed to a 300PR validated field.

[0087] Figure 4 illustrates in dashed box 41 how nonces are generated and in dashed box 43 how the issuing of an elecronic ticket can be requested.

[0088] Before a ticket is requested, at least one nonce 704 has been generated. This is illustrated in more detail in dashed box 41. The nonces are generated by trusted agent 254 responsive to message M401 which is generated in preparation step L10 by the ticket application 200.

[0089] Responsive to the receiving of message 401, to trusted agent 254 initiates processes described in step L11 for generating nonces. In step L11 the trusted agent 254 performs substeps L112-L116.

[0090] In step L112 a nonce 727 is generated, preferably by using a random number generator located in the security element 252. Nonces 727 can also be understood to correspond to unique identifiers (such as URI), and they need not be generated by a random number generator but may also obtain sequential values.

[0091] In step L113 each nonce 727 is stored in a nonce field 726 of registers 724 of the registry 722. This has already been described in more detail with reference to Figures 2B and 2C. The copy of processed nonce 727 is processed to processed nonce 727' and stored together with other similarly processed nonces to form the processed nonces table 730.

[0092] In step L114 a copy of each nonce 727 contained in the registry 722 is processed. Consequently, each nonce is by processing implicitly linked to the trusted agent 254. This can be done by signing each nonce 727 with the trusted agent signature 709 to obtain a processed nonce 727'.

[0093] In step L115 processed nonces 727 are sent to the ticket storage 230 in message M403 and stored into processed nonces table 730.

[0094] In step L116 the trusted agent 254 sends a confirmation message M405 to the ticket application 200 in order to indicate that the execution of process L11 has been finished. The step L10 is terminated upon receiving confirmation message M405.

[0095] Dashed box 43 shows how the issuing of an elecronic ticket can be requested. In step L12 a request M411 is generated and finally sent to the ticket issuing system 101. The ticket application 200 accesses the area of the ticket storage 230 where the processed nonces 727' are stored by sending a message M407 to ticket storage 230, and gets as response message M409 list a processed nonce 727'. The processed nonce 727' is written into the request M411 as well the PKI certificate of the trusted agend 254. Then the ticket application 200 uses available sending means 262 for sending request M411 to the ticket issuing system 101. M411 can also include information on the desired ticket but it does not need to include such information, because the address of the ticket issuing system 101 can do that, such as when the kind of the ticket is designed by a MSISDN number to which the message M411 is sent as an SMS.

[0096] The ticket issuing system 101 recognises that the incoming message M411 is a ticket request and in step K1 the substeps K11 to K13 are performed. In step K11 the ticket issuing system 101 verifies the signature of the processed nonce 727' included in message M411 by using the public key of the trusted agent 254 included in the trusted agent 254 certificate. The certificate need not be there, because instead of transferring a certificate in message M411, a Universal Resource Indicator URI referring to an address location where the certificate is stored. Using the URI the ticket issuing system 101 can find the correct certificate in the Internet 100B or elsewhere.

[0097] In step K12 the ticket issuing system 101 generates an electronic ticket 300. A ticket product tag 721 is included inside the element PTD information 703. This is done in order to facilitate the fast searching of tickets during ticket use; this is in more detail described with reference to Figure 6A.

[0098] Further, the ticket issuing system 101 also embeds or sets a reference in the element PTD information 703 to the ticket object 303. The ticket object 303 may include, in any way acceptable by parsing means 811 of the ticket inspection system 106, TUID 702. In practice, the TUID 702 should be the same as the TUID 702' inside ticket data 706.

[0099] Further, in step K12 the processed nonce 727' is stored among processed nonces table 730 that was provided by the ticket application 200 in M411 is verified by the ticket issuing system 101. Then the copy of nonce 727 is written inside the ticket data 706 i.e. into the field nonce 704 as shown in Figure 3B.

[0100] In step K13 the ticket issuing system 101 seals the electronic ticket 300. This was illustrated in more detail in Figure 3B by defining public part 300PU and private part 300PR for the electronic ticket 300.

[0101] Further, in step K13 the ticket issuing system 101 signs the private part 300PR with issuer signature 708 and encrypts the ticket data 706 with the public key of the trusted agent 254, thus generating the ticket data 706.

[0102] The ticket issuing system 101 can embed the private part 300PR inside the ticket application information 302 of the electronic ticket 300, or it can insert a link into ticket application inofmation 302 pointing or referring to a separate object.

[0103] After performing steps K11 to K13, the ticket issuing system 101 sends the sealed ticket in message M413 to be available for the ticket application 200, i.e. to the mobile device 102. The mobile device 102 using its receiving means 263 passes the message M413 to the ticket application 200, for example, by notifying a suitable port daemon.

[0104] The ticket application 200 receives message M413 including an electronic ticket 300 in sealed state. The message M413 comprises at least some of the following: product tag 721, ticket unique identifier 702, and a value for the nonce 704. After receiving the message M413, the ticket application 200 indicates the reception of the electronic ticket 300 to the user by the use of input/output means 260. The user can then choose whether to accept or discard the electronic ticket 300. If the user accepts the ticket, the ticket application 200 in step L13 stores the electronic ticket 300 in sealed form ticket by sending the message M415 to the ticket storage 230.

[0105] Figure 5 shows the registration of the electronic ticket 300 which is in sealed state. At any given time after the phase of delivery, the user can choose to register the electronic ticket 300 with the trusted agent 254. According to the present invention, a delayed validation of the electronic ticket 300 can thus be achieved. The process of registering a ticket includes can be carried out as follows.

[0106] In step L14 an electronic ticket 300 is selected. In order to facilitate the selection, the user can employ the U/I part 201 of the ticket application 200 or the mobile device 102 in order to access the ticket storage 230 and select an electronic ticket 300 which is in sealed state. The ticket application send message M501 to ticket storage 230 which returns returns the electronic ticket 300 in sealed state in message M503.

[0107] Next the ticket application 200 proceeds to step L15A where a ticket validation request M505 is generated. In the ticket validation request M505 the ticket application 200 sends the electronic ticket 300 in sealed form together with the issuer certificate to the trusted agent 254. In response to receiving the ticket validation request M505 the trusted agent performs in step L15B substeps L151 to L156. In step L151 the trusted agent 254 decrypts ticket data 706' using its dedicated private key, and thus obtains the ticket data 706. Further, in step L152 the trusted agent 254 compares the issuer signature 708' with the ticket data 706. If the comparison result shows that the issuer signature 708' does not match with the ticket data 706, an error message is generated and no further steps are performed in the trusted agent.

[0108] In the opposite case, if the comparison result of the step L152 was successful, in step L153 the trusted agent 254 compares the nonce 704 inside the ticket data 706, with the available nonces inside the registry 722 as already shown in Figure 2B. If the comparison result shows that a matching nonce is found, the registering of the ticket is allowed.

[0109] In step L154 the trusted agent 254 copies the TUID 702' into the inside of the TUID field 725 corresponding to the nonce field 726 containing the matching value of nonce 704.

[0110] In step L155 the trusted agent 254 signs ticket data 706 with its own trusted agent signature 709. In the signing it may then use its dedicated private key.

[0111] In step L156 the trusted agent 254 returns the private part 300PR to the ticket application 200 by sending it in the message M507.

[0112] In response to receiving the message M507, the ticket application 200 sends the electronic ticket 300 in validated state to the ticket storage 230.

[0113] Figures 6A and 6B illustrate one aspect of the present invention. It is assumed that the inspection system corresponds to that of Figures 1B and 1C as described above. The proximity detection means 802 and proximity discrimination means 803 are used in the case of a local presentation of the electronic ticket 300.

[0114] In step K4 the ticket inspection system 106 sends a message M601 to the ticket application 200. The message M601 includes product tag 721 for the service that is being offered through the ticket inspection system 106, and a new value NONCE" for the nonce 704. The ticket inspection system 106 stores a copy of the new value NONCE" for the nonce 704 in storage 807 so that the private part 300PR in validated state defined by this new value NONCE" for the nonce 704 can be verified during the ticket verification phase in steps K15-K20 of Figure 6B.

[0115] The new value NONCE" for the nonce 704 is preferably unique for each ticket use request M601. The preferred method to generate this new value NONCE" for the nonce 704 is to use a random number generator for generating random digits, consisting of 64 or 128 bits, for example.

[0116] It is also assumed that the ticket inspection system 106 is able to discriminate between mobile devices 102, with the help of its proximity detection means 802, and/or its proximity discrimination means 803.

[0117] The ticket application 200 receives the message M601 via receiving means 263. In response to receiving the message M601, after processing the message, the ticket application 200 searches in step L16 through the ticket storage 230 for tickets matching the product tag 721 included in the message M601 by sending a message M603. More precisely, the searching is performed in the field product tag 721 of the tickets 300 as described in Figure 3A. If among the tickets 729 there are any or some ticket electronic ticket 300 corresponding to the field product tag 721 contained in message M601, the ticket storage 230 returns the TUID of them in message M605.

[0118] In step L17, the ticket application 200 displays the results of the search on the display 261.

[0119] In step L18 in the case that there were several tickets matching the product tag supplied by the inspection system 106, the user is allowed to select one to be used. The ticket application 200 communicates the selection by sending message M607 to the ticket storage 230 which in message M609 returns the TUID and NONCE' of the electronic ticket 300 which is in validated state, i.e. it has been registered with the trusted agent 254 earlier.

[0120] In step L19A message M611 is first generated in the ticket application and then sent to the trusted agent 254. The message M611 includes the new value NONCE" of the nonce 704 and the private part 300PR of the selected electronic ticket 300 in validated state. In response to receiving message M611, several substeps L191 to L195 are performed at the trusted agent 254 in step L19B.

[0121] In step L191 the trusted agent 254 compares its own trusted agent signature 709 with the ticket data 706 included in message M611. In step L192 the trusted agent searches in the registry 722 the individual registers 724 until it finds one such register 724 for which ist TUID field 725 includes a matching value for the TUID 702 in the ticket data 706.

[0122] When an adequate register 724 is found, the trusted agent 254 compares the values of the nonce field 726 with the nonce 704 to verify that they match. This is done in order to verify that the version of the private part 300PR of the electronic ticket 300 in validated state presented to the trusted agent 254 is the latest one.

[0123] In step L193, if steps L191 and L192 were successfully performed, and assuming that N of uses 711 shows that the ticket has a number of uses left different from zero, the trusted agent 254 updates the N of uses 711 to correspond to number of uses left. This can be done by changing the ticket data 706 by subtracting a predefined value from it, such as N is changed to a value N-1 if the predefined value is 1.

[0124] In step L194 the trusted agent 254 updates with the new nonce provided by the inspection system 106 the values of the nonce fields of: i) in the ticket data 706, the nonce 704; and ii) in the corresponding register 724 the corresponding nonce 727 in nonce field 726. This is the corresponding register 724 to the TUID field 725 containing a matching value to the value contained in the TUID 702' of the ticket data 706.

[0125] If the N of uses 711 matches with a predefined criteria, such as when the current number of uses left for the ticket after step L193 would be zero, the trusted agent 254 removes from the registry 722 the register 724 the TUID field 725 of which contains a value matching with the TUID 702' in the ticket data 706.

[0126] In step L195 the trusted agent 254 signs the newly modified private part 300PR validated, and returns it to the ticket application 200 in message M613.

[0127] At the last part of step L19A, the ticket application 200 stores the new version of the electronic ticket 300 in the ticket storage 230 in message M615.

[0128] In step L20 the ticket application 200 creates message M617 including the corresponding ticket object 303, of the PTD information 703 of the electronic ticket 300, and the new version of the private part 300PR of the electronic ticket in validated state. Then the message M617 is sent to the inspection system 106.

[0129] Figure 6B illustrates a scenario of using an electronic ticket 300, or how an electronic ticket 300 is verified in step K5.

[0130] In response to receiving a message M619 the ticket object 303 and the new version of the validated private part 300PR via receiving means 806, the ticket inspection system 106 verifies in step K15 that the ticket object 303 has not been tampered with.

[0131] If the selected verification method is that the ticket object 303 has been digitally signed with the issuer signature 708, the execution of step K15 requires that the inspection system 106 performs the verification of the issuer signature 708 over the ticket object 303. Hence, the inspection system 106 needs to have prior access to the ticket issuing system 101 PKI certificate. It is assumed that the inspection system 106 already has this information, and thus the mobile device 102 does not need to provide it. Preferably, the inspection system 106 extracts from the ticket object 303 the value of TUID 702.

[0132] In step K16 the inspection system 106 verifies the trusted agent signature 709 by comparing it with the ticket data 706. For this purpose it uses the trusted agent 254 certificate which has been preferably delivered in step L20.

[0133] In step K17, if the verification result of step K6 shows that the trusted agent signature 709 matches with ticket data 706, i.e. that the step K16 was successful, the inspection system 106 compares the nonce 704 of the private part 300PR in ticket data 706 with the copy of the new nonce NONCE" sent to the ticket application 200 in step K14. This step can be perormed in a number of ways, for instance, by making a search for the nonce 704, in storage 807 of the inspection system 106.

[0134] In step K18, if the result of step K17 shows that step K17 was successful, i.e. if the nonce 704 of the ticket data 706 matches with the copy of the new nonce sent to the ticket application 200, the inspection system 106 compares the TUID 702 of the ticket object 303 with TUID 702' of the private part 300PR in order to verify that they are related.

[0135] In step K19 the inspection system 106 grants the user access to a given service. This can be performed by opening a gate, by changing a state of a system flag in a computer memory, by sending a message, or by showing a positive acknowledgement signal to a human inspector, for example.

[0136] In step K20 the inspection system 106 generates a confirmation message M621 to be sent to the ticket application 200. This confirmation message M621 preferably contains a time stamp and an ticket product tag. Then the confirmation message M621 is sent from the ticket inspection system 106 to the ticket application 200.

[0137] In step L21, in response to receiving of the confirmation message M621, the ticket application 200 indicates the receiving of the confirmation message M621 to the user using suitable presenting means 260B using the U/I part

201. The user can then by using receiving means 263, such as by giving his/her input via the keyboard, a joystick or by using a voice command decide to store the confirmation message M621 in the ticket storage 230. The confirmation message M621 can be used as a receipt, i.e. it serves in proving that the user had access to the service in a correct manner. If the message M621 is to be stored as a confirmation message, the ticket application 200 saves it into the ticket storage 230.

[0138] Figure 7 shows a scenario of transferring an electronic ticket 300, the transferring including also steps for ticket verification. A user with a mobile device 102B requests the user with a mobile device 102 to transfer a given number of ticket units of a given multiple use ticket to the device 102B. For the sake of clarity, in the nomenclature similar references are used in such a manner that the blocks in the device requesting the ticket units is denoted with adding a capital letter B to the end of each reference.

[0139] A transfer action of this kind is up to a high extent analogical to transfer a single unit ticket completely to the other device.

[0140] In step L22 the ticket application 200B requests processed nonces 727' stored in processed nonces table 730 that are available by sending a message M701 to ticket storage 230B. In response to message M701, at least one non-used processed nonce 727' having a value NONCE" is received from the ticket storage 230B in message M703. The processed nonce 727' is sent in a message M705 to another mobile device 102 which routes the message M705 to the ticket application 200. Preferably, the message M705 also contains the trusted agent 254B PKI certificate.

[0141] The ticket application 200B in step L22 marks the nonce 704 in the ticket storage 230B used.

[0142] In step L23 the ticket application 200 stores the processed nonce 727' obtained in message M705 into the ticket storage 230 as well as the trusted agent 254B PKI certificate. Preferably, the ticket application 200 allows via the U/I part 201 the user to give a user-defined label to processed nonce 727' to indicate its origin and/or future use (e.g. "Ticket4Lorena"). In addition, signed nonce values from other devices can be stored in a particular area of the ticket storage 230 in order to achieve a better user experience. Furthermore, the ticket application 200 establishes a reference link between this signed nonce 704 and the trusted agent 254B PKI certificate in order to facilitate later processes.

[0143] Later, in step L24A, the user decides to split the electronic ticket 300, so he or she uses the U/I part 201 of the ticket application 200 to initiate a split process. This process starts by allowing the user to select i) the processed nonce 727' which is easy to recognise because of the user-defined label, and ii) the electronic ticket 300 to be split. Also, the user can use the U/I part 201 for determining how many units are to be split. The items to be selected are requested by sending message M709 to ticket storage 230 which then in messages M711 to M715 responds to the message M709. Message M711 includes processed nonces 727' including values NONCE", message M713 includes electronic tickets 300 in validated form, including TUID and NONCE', whereas message M715 includes the trusted agent 254B PKI certificate.

[0144] Consequently, values retrieved in messages M711 to M715 are passed to the trusted agent 254 in message M717 together with the number of units value selected by the user.

[0145] In response to the receiving of message M717, in step L24B several substeps L241 to L248 are performed in the trusted agent 254. In step L241 the trusted agent 254 verifies the NONCE" signature in processed nonce 727' using the trusted agent 254B public key contained in the trusted agent 254B PKI certificate.

[0146] In step L242 the trusted agent 254 verifies its own trusted agent signature 709 over the ticket data 706. In step L243, if the results of steps L241 and L242 have been successful, the trusted agent 254 searches in the registry 722 through the individual registers 724 until it finds the one the TUID field 725 of which contains a matching value for the TUID 702' in the ticket data 706.

[0147] When an adequate register 724 is found, the trusted agent 254 compares the values of the nonce field 726 with nonce 704 to verify that they are identical. This is done in order to verify that the version of the validated private part 300PR presented to the trusted agent 254 is the latest one.

[0148] In step L244 the trusted agent 254 generates ticket data 706B by: i) creating fields TUID 702B', nonce 704B, and N of uses 711B, ii) copying TUID 702' of ticket data 706 into TUID 702B' of ticket data 706B , iii) copying NONCE" to the nonce 704B in the ticket data 706B, and iv) copying the value of number of units to split to the N of uses 711B.

[0149] In step L245 the trusted agent 254 updates the N of uses 711 with the new value in ticket data 706, such as "N-n of units to split".

[0150] In step L246 the trusted agent 254 updates the values of the nonce 704 and of the nonce field 726.

[0151] To summarize: In the case that the number of units left (N-n of units split) is different from zero, the trusted agent 254 generates a new nonce value and inserts it as the value of the nonce 704 in the private part 300PR in ticket data 706 and the corresponding nonce field 726 in the registry 722.

[0152] In the case that the number of units left (N-n of units split), is equal to zero corresponding to the case that all units have been transferred to the other ticket, the trusted agent 254 removes from the registry 722 the corresponding register 724 whose TUID field 725 contains a matching value for the TUID 702' in the ticket data 706.

[0153] In step L247 the trusted agent 254 seals private part 300PRB by signing it with its own trusted agent signature

709" and encrypts the private part 300PRB in ticket data 706B with the trusted agent 254B public key, thus generating ticket data 706'B.

[0154] In step L248 the trusted agent 254 signs the validated private part 300PR with its own trusted agent signature 709.

[0155] Finally, the trusted agent 254 returns in message M719 the private part 300PRB in sealed state and private part 300PR in validated state to the ticket application 200 which stores the tickets in the corresponding compartments in the ticket storage 230 by sending message M721.

[0156] In addition, the ticket application 200 stores the private part 300PRB with the same user-defined label. For enhanced usability, the storage area in the ticket storage 230 for these split tickets from/to other devices can be tailored device-specifically. A duplicate of the original public part of electronic ticket 300PU can be stored with the private part of electronic ticket 300PRB, or a link to it can be provided. In the latter case, the duplication of the public part of electronic ticket 300PU is performed during the transfer of the electronic ticket 300B.

[0157] In step L25, at some given time, the user decides to send the sealed electronic ticket 300B (300B = 300PUB + 300PRB) to the other mobile device 102B. Thus, he or she uses the U/I part 201 for selecting a sealed ticket, requesting it from the ticket storage 230 by sending message M723 and receiving it in message M725. Then the electronic ticket 300B in sealed state is sent to the other mobile device 102B in message M727.

[0158] In step L26 the ticket application 200B receives the ticket in message M727 via receiving means 263B. With its input/output means 260B, in response to receiving to the ticket, the ticket application 200 indicates to the user the reception of a digital ticket. The user can choose to accept or discard the electronic ticket 300B received. If the he or she accepts the ticket, the ticket application 200B stores the sealed ticket in the ticket storage 230B by sending message M729.

[0159] The different steps of Figures 4 to 7 can be implemented as primitives of a smart card or a secure element which enables then a high level of code reuse.

[0160] The type of services offered by digital tickets can also be different from the typical services directly offered to users, such as transportation tickets. Alternative services can include the execution of content stored in the inspection system 106 or elsewhere, for the benefit of the user or some other entity.

[0161] Although in the examples it is assumed that the presentation environment of the ticket object to the inspector in the preferred embodiment would be either remote (e.g. at the Internet 100B) or local (e.g. at a transportation service access point by local transportation means such as BLUETOOTH or IrDA), with special emphasis in the local environment, the present invention does not exclude the personal presentation environment that is around the mobile device 102 itself. This personal presentation environment can be an element permanently integrated by software, hardware, or both in the mobile device 102 and/or located in a detachable separate hardware component.

[0162] Usually, copy protection is relevant only on the context of double spending of the same ticket object 303. In the present invention the copy protection is achieved by rendering useless copies of the ticket object 303 that are not validated by a trusted agent through a reliable and protected interface, such as by using private part of electronic ticket 300PR.

[0163] The present invention is mainly but not exclusively meant for electronic tickets. There are other types of data objects benefitting from such a high-level security copy-protection offered by the present invention, requring only little or even none modification. To such types of data objects belong medical prescriptions, legal documents, and even executable content. In particular, in the last aforementioned case the presentation enviroment of the object can be either remote, local, or personal, as already discussed.

[0164] Although the invention was described above with reference to the examples shown in the appended drawings, it is obvious that the invention is not limited to these but may be modified by those skilled in the art without difference from the scope and the spirit of the invention.

List of used references

[0165]

41	nonce generation
43	ticket issuing request
100A	mobile network
100B	the Internet
101	ticket issuing system
1011	front end of ticket issuing system
1012	back end of ticket issuing system
1013	data storage of ticket issuing system
102, 103	mobile devices

104	personal computer
105	ticket printer
106	inspection system
199	shielding means
200	ticket application
201	user interface part of the ticket application 200
202	parsing means
204	comparison means
206	generation means
224	simple ticket security means
230	ticket storage
250	security means
252	security element
254	trusted agent
260	input/output means
260B	presenting means
261	display
262	sending means
263	receiving means
264	loudspeaker
265	radio frequency tag
280	validating means
300	electronic ticket
300PU	public part of electronic ticket
300PR	private part of electronic ticket
301	user information
302	ticket application information
303	ticket object
701	security element information
702	ticket unique identifier TUID
703	PTD information
704	nonce
705	presentation information
706	ticket data
707	security information
708	issuer signature
709	trusted agent signature
711	N of uses
720	ticket value data
721	product tag
722	registry
723	ticket application system
724A,B,C	register 1,2,3
725A,B,C	TUID field
726A,B,C	nonce field
727	nonce
727'	processed nonce = 727 + 709 calculated for 727
729	tickets
730	processed nonces table
731	signature element
801	broadcasting means
802	proximity detection means
803	proximity discrimination means
804	point to point sending means
805	transport means
806	receiving means
807	storage
808	generation means

809	comparison means
810	verification means
811	parsing means
814	ticketing means
ΔR_1, ΔR_2	proximity range of inspection system 106

Claims

1. A device for validating an electronic ticket, **characterised in that** it includes:

   - receiving means (263) for receiving an electronic ticket (300), the electronic ticket (300) including a first identifier (TUID) and a second identifier (NONCE');
   - a ticket storage (230) for storing the electronic ticket (300);
   - secure storing means (252) for storing the first identifier (TUID1) and the second identifier (NONCE'); and
   - validating means (280) adapted to store the first identifier (TUID1) to the secure storing means (252) when the electronic ticket (300) is validated.

2. A device according to claim 1, **characterised in that** it further includes security means (250) for verifying the origin of the electronic ticket (300), preferably by verifying a digital signature in at least a part of ticket (300PR) including said first and second identifiers (TUID1, NONCE'), especially using a private key assigned to a trusted agent (254).

3. A device according to claim 2, wherein: the security means (250) are adapted to decrypt a ticket part (303) containing said first and second identifiers (TUID, NONCE).

4. A device for presenting an electronic ticket (300), especially a device according to any one of claims 1, 2, or 3, **characterised in that** it includes: presenting means (260B) for presenting the first identifier (TUID1), the second identifier (NONCE'), and a ticket object (303) in order to use said electronic ticket (300).

5. A device according to claim 4, **characterised in that**: the device includes means (204) for verifying the identity of an entity (106, 105) to which the electronic ticket is going to be presented.

6. A device according to any one of the preceding claims, **characterised in that** the device further includes: means (254) for changing a third identifier (711) in the ticket data (706) in response to a change request (M601), especially relating to said using or transfer of the electronic ticket, or in response to using the ticket, such as received from an entity (105, 106) to which the electronic ticket (300) is presented.

7. A device according to any one of the preceding claims, **characterised in that** the device further includes:

   - generation means (206) adapted to generate a second identifier (727);
   - generation means (206) adapted to generate a ticket issuing request (M411) including the processed second identifier (727') generated; and
   - sending means (262) for sending the ticket issuing request (M411) to a ticket issuing system (101).

8. A device according to claim 7, **wherein:** the ticket issuing request (M411) further includes an agent certificate (709).

9. A device according to any one of claims 6 to 8, wherein: the ticket storage (230) and/or the secure storing means (252) are adapted to store a new second identifier (NONCE') received from an entity (105, 106) to which the electronic ticket (300) is presented.

10. A device according to claim any one of the preceding claims, wherein: the device includes security means (252) adapted to sign the second identifier (NONCE') with an agent private key (709) prior to sending the electronic ticket issuing request by the sending means (262).

11. A device according to any one of claims 1-10, wherein: the second identifier (NONCE', NONCE") is stored in the secure storing means (252), and the processed second identifier (727') is stored in the ticket storage (230).

12. A ticket issuing system (101) or a device for issuing an electronic ticket (300), wherein the improvement comprises:

the system (101) or the device includes generation means (1012) adapted to generate an electronic ticket (300) responsive to a request (M411), the request (M411) including a first identifier (TUID1) and a second identifier (NONCE'), especially when the request (M411) has been generated by a device (102) according to any one of the previous claims; and where the electronic ticket (300) includes a first identifier (NONCE') or an identifier derived therefrom.

13. A system or device according to claim 12, wherein: the system or device includes means (1012) for sealing the ticket (300).

14. A device (105, 106) for requesting the use of an electronic ticket (300), wherein the improvement comprises: the device includes generation means (808) for generating a request (M601) for using an electronic ticket (300), the request (M601) including a refresh value (NONCE") for a second identifier (704) of said electronic ticket (300).

15. A system wherein a device (102) for validating an electronic ticket (300), a ticket issuing system (101) and/or a device for issuing an electronic ticket (300), and a device (105, 106) for requesting the use of an electronic ticket (300) is used.

16. A method for validating an electronic ticket, **characterised in that** it includes the steps of:

- receiving an electronic ticket (300), the electronic ticket (300) including a first identifier (TUID) and a second identifier (NONCE');
- storing the electronic ticket (300);
- storing the first identifier (TUID1); and
- storing the first identifier (TUID1) to secure storing means (252) when the electronic ticket (300) is validated.

17. A method for presenting an electronic ticket (300), especially in connection with the method of claim 19, **characterised in that** it includes the step of: presenting the first identifier (TUID1) and the second identifier (NONCE') in order to use said electronic ticket (300).

18. A method for issuing an electronic ticket (300), comprising the step of: generating an electronic ticket (300) responsive to a request (M411) including a first identifier (TUID1) and a second identifier (NONCE'), especially when the request (M411) has been generated using a method according to any one of the previous claims; and where the electronic ticket (300) includes a first identifier (NONCE') or an identifier derived therefrom.

19. A method for requesting the use of an electronic ticket (300), comprising the step if: generating a request (M601) for using an electronic ticket (300), the request (M601) including a refresh value (NONCE") for a second identifier (727) of said electronic ticket (300).

20. A method according to claim 19, further comprising the step of: presenting a product tag (704) as a response of detecting a mobile device by the proximity detection means (802).

21. A method according to claim 19 or 20, further comprising the step of: in response to detecting a mobile device by the proximity detection means (802), presenting a request (M601) for using an electronic ticket (300).

22. A mobile device, especially a mobile phone, wherein: a device or method according to any one of the preceding claims is used.

23. A mobile device according to claim 22, wherein: the mobile device includes a ticket application (200) or ticketing means (814).

24. A mobile device according to claim 23, wherein: the ticket application (200) or ticketing means (814) comprises software code programmed in a symbolic language, especially using any JAVA compiler.

25. A mobile device according to claim 24, wherein: the software code shares object classes between functionalities for ticket transferring and ticket issuing request, especially JAVA classes.

26. An electronic ticket (300) having a sealed state and a validated state, wherein the state of the electronic ticket (300) is defined by the public part (300PU) or private part (300PR) of the electronic ticket (300), in such a manner

that whenever the private part (300PR) corresponds to a valid value, the ticket is in the validated state.

27. An electronic ticket (300) as defined in claim 26, wherein: the valid value for private part (300PR) corresponds to an identifier (704) stored in security means (250) of a mobile device.

Amended claims in accordance with Rule 86(2) EPC.

1. A device (102) for ordering and validating an electronic ticket (300), the device (102) comprising: a ticket application (200); a security element (252); a trusted agent (254); a registry (722); a ticket storage (230); and sending and receiving means (262, 263); **characterized in that:**

- the trusted agent (254) is adapted to generate a random identifier (727); and to store said random identifier (727) in the registry (722) and after signing as a signed random identifier (727') in the ticket storage (230);
- the ticket application (200) is adapted to: generate a request (M411) for an electronic ticket (300), the request (M411) comprising said signed random identifier (727'); and to send said request (M411) to a ticket issuing system (101) using the sending means (262);
- the trusted agent (254) is adapted to check the integrity of an electronic ticket (300) received in sealed state by the receiving means (263) from the ticket issuing system (101);
- the ticket application (200) is adapted to compare an identifier (704) in the electronic ticket (300) with the random identifiers (727) stored in the registry (722), if the outcome of the integrity check was positive;
- the trusted agent (254) is adapted to: copy a ticket unique identifier (702') into a ticket unique identifier field (725) corresponding the identifier (727), if an identifier (727) corresponding the identifier (704) was found; and to sign a ticket data field (706) of the electronic ticket (300), thereby changing the electronic ticket (300) from sealed state into validated state; and
- the ticket application (200) is further adapted to: send the electronic ticket (300) in validated state into the ticket storage (230).

2. A device (102) of claim 1, further **characterized in that**: the trusted agent (254) is adapted to:

- decrypt a ticket data field (706') using its dedicated private key;
- compare an issuer signature (708') with the ticket data (706); and
- to compare an identifier (704) inside the ticket data (706) with the available random identifiers (727) stored in the registry (722), if the issuer signature (708') matches with the ticket data (706); and further to sign the ticket data (706) with a trusted agent signature (709).

3. A device (102) of claim 1 or 2, wherein: said random identifier (727) is a random number.

4. A ticket issuing system (101) comprising: means (1011, 1012, 1013) adapted to:

- receive a request (M411) for an electronic ticket (300), the request (M411) comprising a signed random identifier (727') from a device (102) for ordering and validating an electronic ticket (300);
- store the signed random identifier (727');
- verify a signature of the signed random identifier (727');
- generate an electronic ticket (300), if the verification shows that the random identifier (727) has been signed by a trusted agent (254), the electronic ticket (300) comprising: a part (300PR) signed by the ticket issuing system (101); further comprising a ticket unique identifier (702") in sealed state; and
- send the ticket to the device (102) for ordering and validating an electronic ticket (300).

5. A ticket issuing system (101) of claim 4, **wherein**: the said random identifier (727) is a random number.

6. An electronic ticket (300), comprising: a random identifier (704), originally comprised in a request (M411) for the electronic ticket (300) as a second random identifier (722), and later generated by: another trusted agent (254) for transferring the ticket and/or a ticket inspector (105, 106) for requesting the use of the electronic ticket (300); the said random identifier (704) being signed:

- (704') by a ticket issuing system (101) when the electronic ticket (300) is delivered to a user terminal (102);
- (704 B') by a trusted agent (254) in a user terminal (102) when the electronic ticket (300) is to be transferred

to another user terminal; and

- (704) by a trusted agent (254) in the user terminal (102) when the ticket has been validated for use.

7. An electronic ticket (300) of claim 6, **wherein:** the said random identifier (727) is a random number.

FIG 1A Prior Art

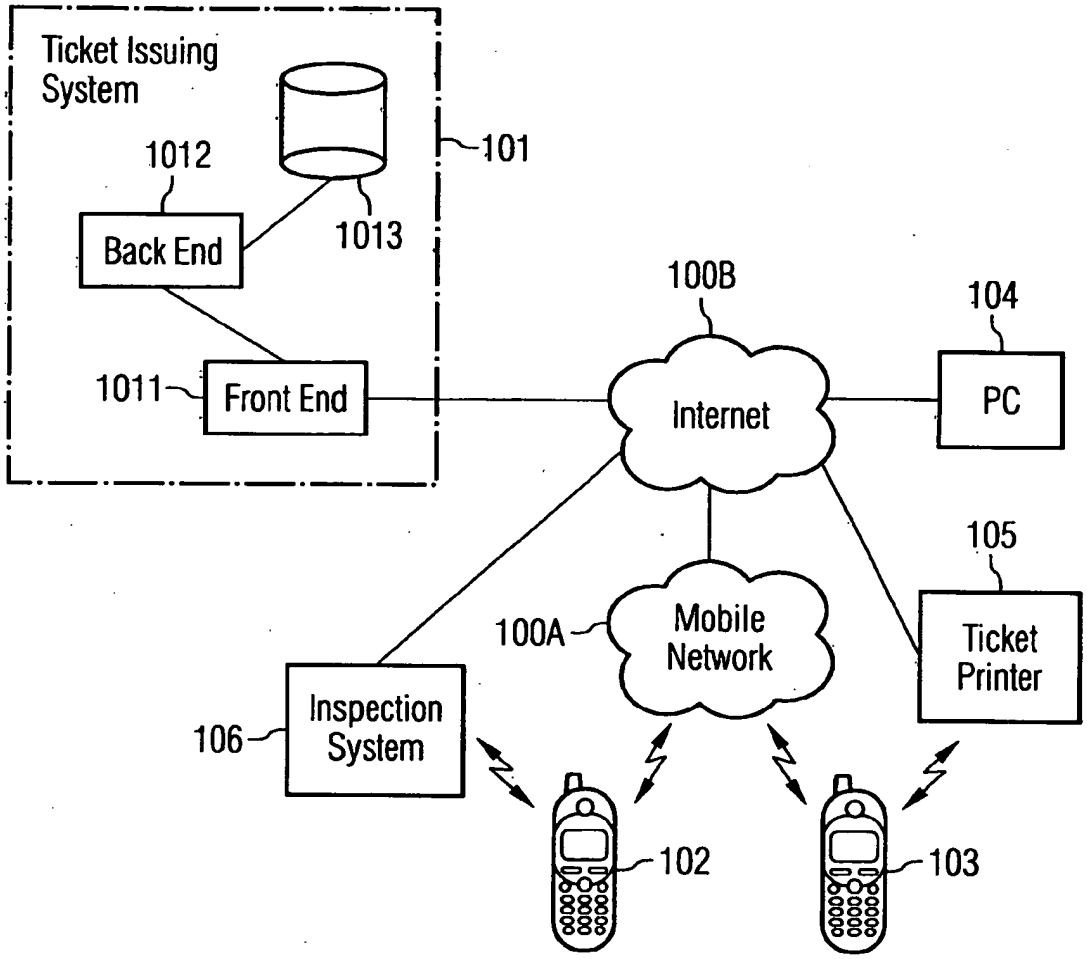
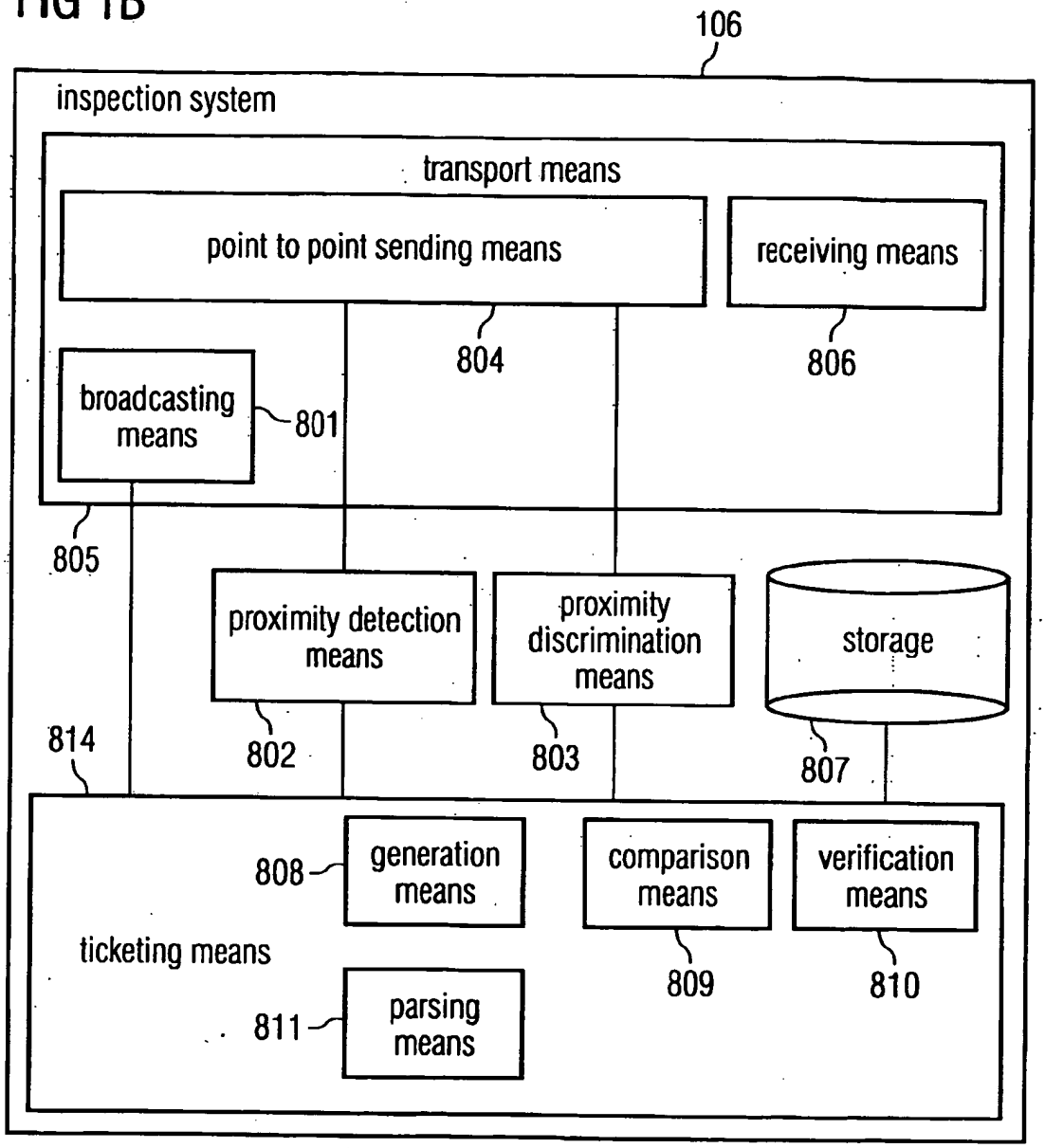


FIG 1B


106
inspection system
transport means
point to point sending means
receiving means
804
806
broadcasting means
801
805
proximity detection means
proximity discrimination means
storage
814
802
803
807
808
generation means
comparison means
verification means
ticketing means
809
810
811
parsing means

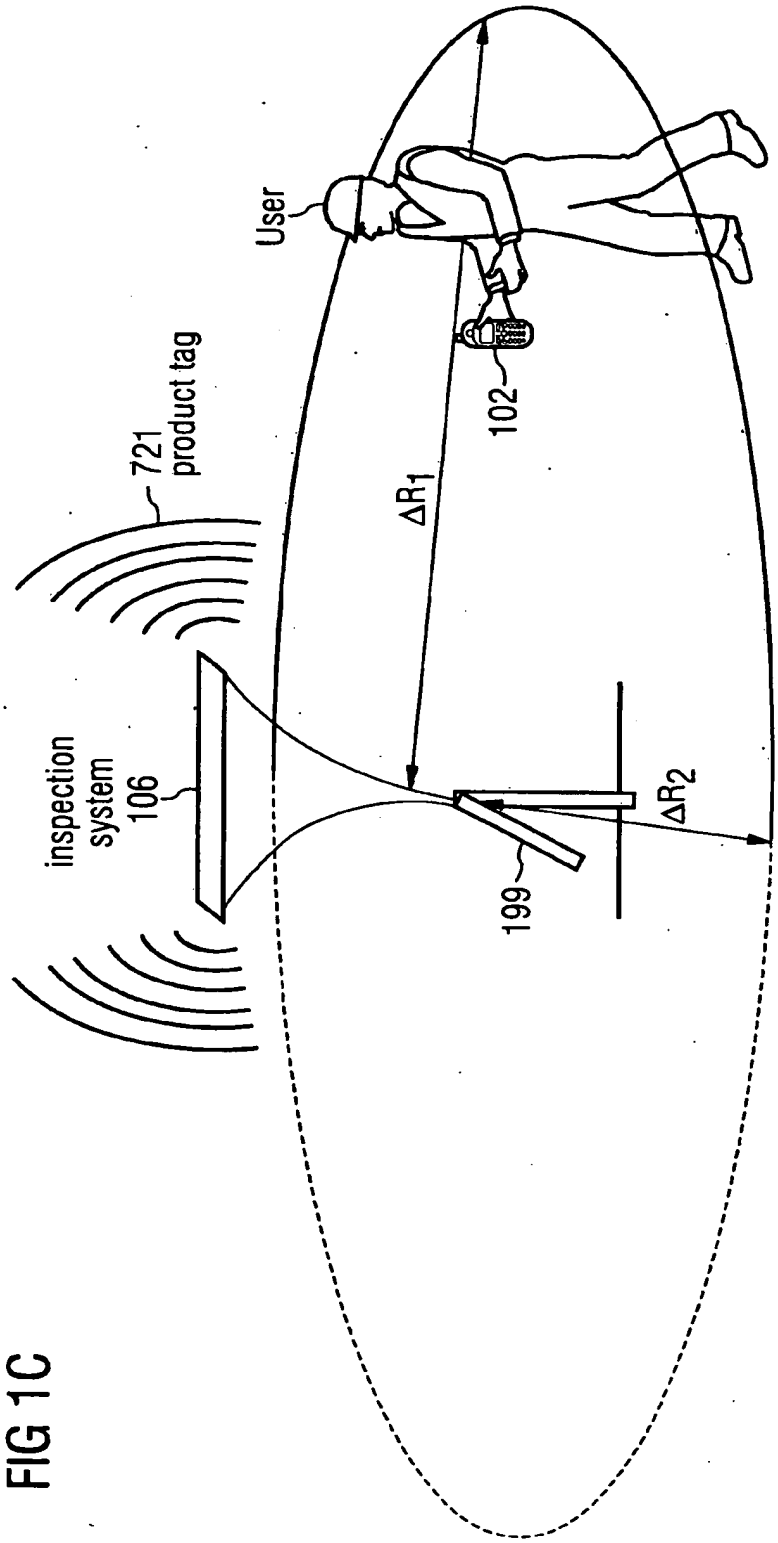
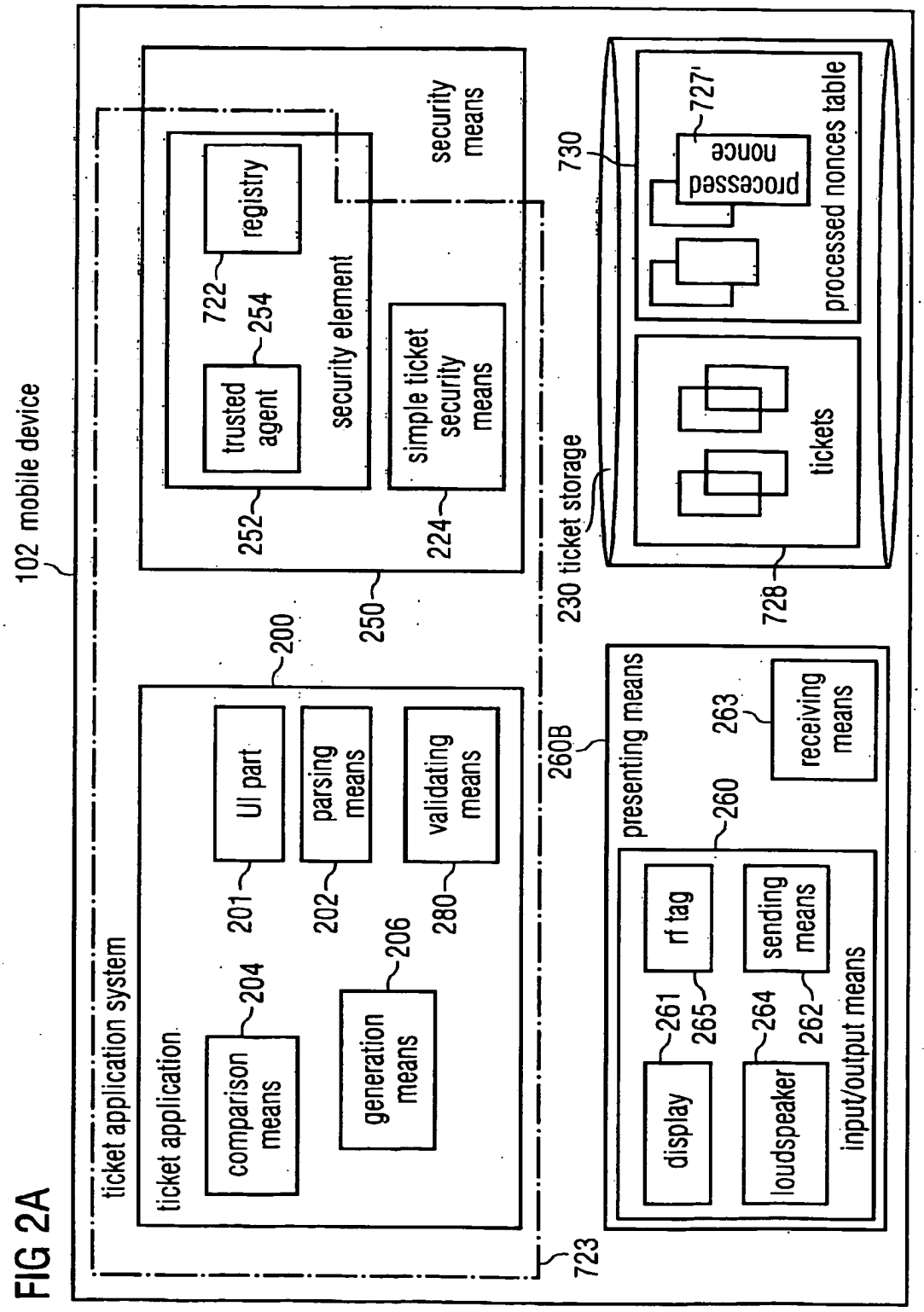

User
102
721
product tag
ΔR_1
inspection
system
106
199
ΔR_2

FIG 1C

FIG 2A


102 mobile device
ticket application system
ticket application
comparison means
204
UI part
201
parsing means
202
generation means
206
validating means
280
200
723
security means
security element
registry
722
trusted agent
254
252
simple ticket security means
224
250
230 ticket storage
730
processed nonces table
processed nonce
727'
tickets
728
260B
presenting means
260
display
261
265
rf tag
loudspeaker
264
sending means
262
input/output means
receiving means
263

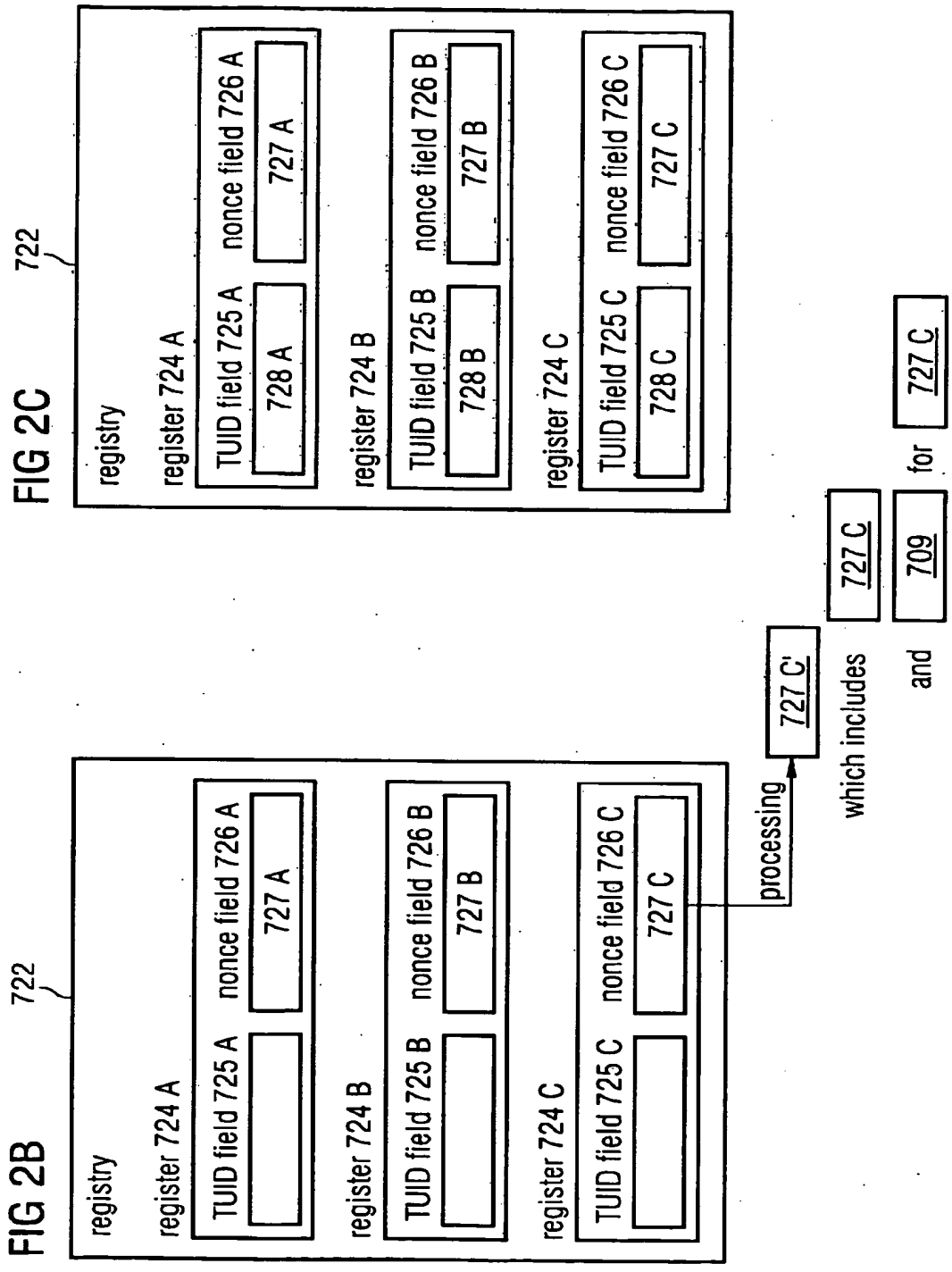


FIG 2B
722
registry
register 724 A
TUID field 725 A
nonce field 726 A
727 A
register 724 B
TUID field 725 B
nonce field 726 B
727 B
register 724 C
TUID field 725 C
nonce field 726 C
727 C
processing
727 C'
which includes
727 C
and
709
for
727 C
FIG 2C
722
registry
register 724 A
TUID field 725 A
nonce field 726 A
728 A
727 A
register 724 B
TUID field 725 B
nonce field 726 B
728 B
727 B
register 724 C
TUID field 725 C
nonce field 726 C
728 C
727 C

FIG 3A

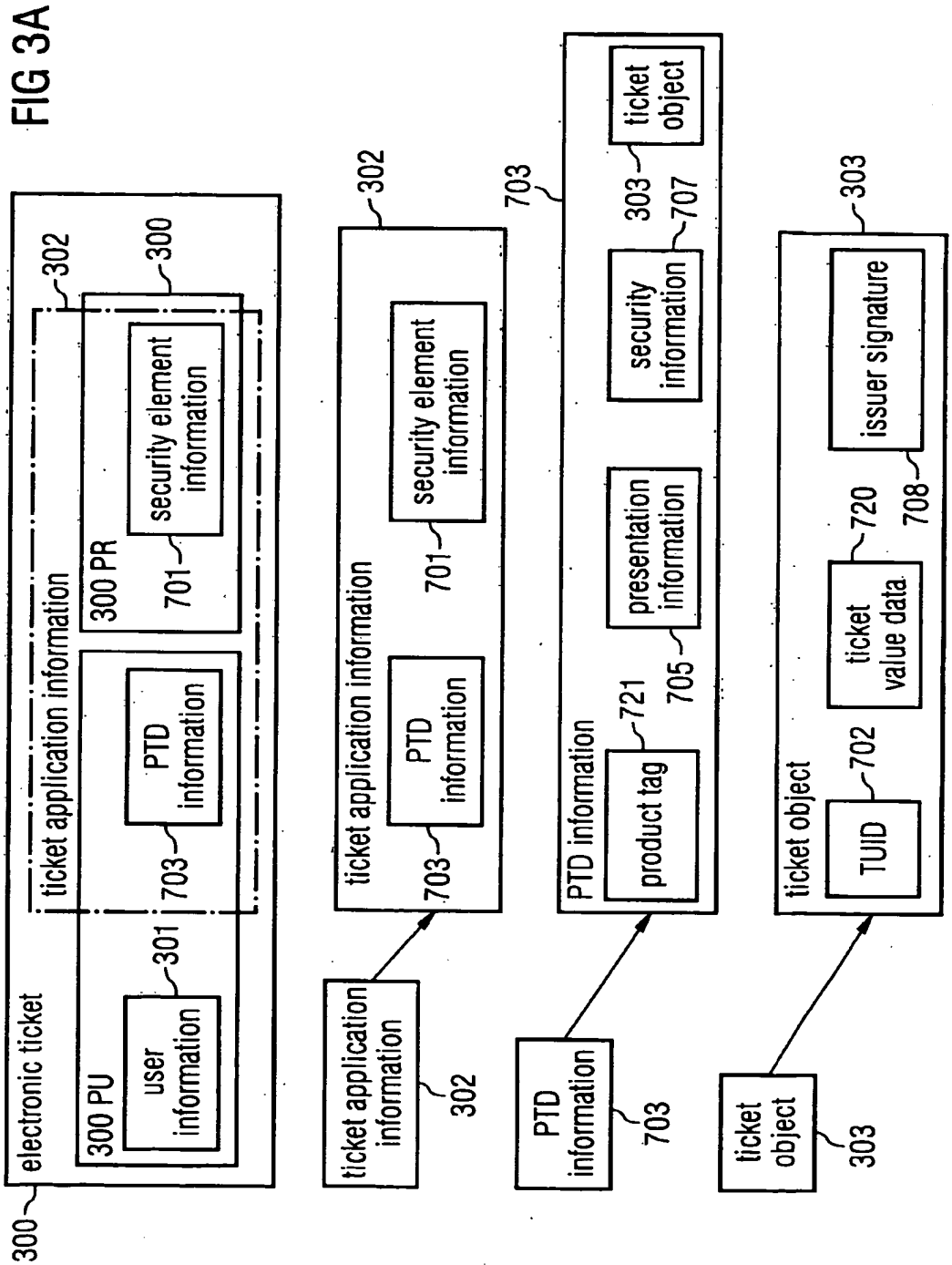

electronic ticket
300
ticket application information
302
300 PU
user information
301
PTD information
703
300 PR
security element information
701
300
ticket application information
302
PTD information
703
security element information
701
ticket application information
302
PTD information
703
PTD information
product tag
721
presentation information
705
security information
707
ticket object
303
703
ticket object
TUID
702
ticket value data
720
issuer signature
708
303
PTD information
703
ticket object
303

FIG 3B

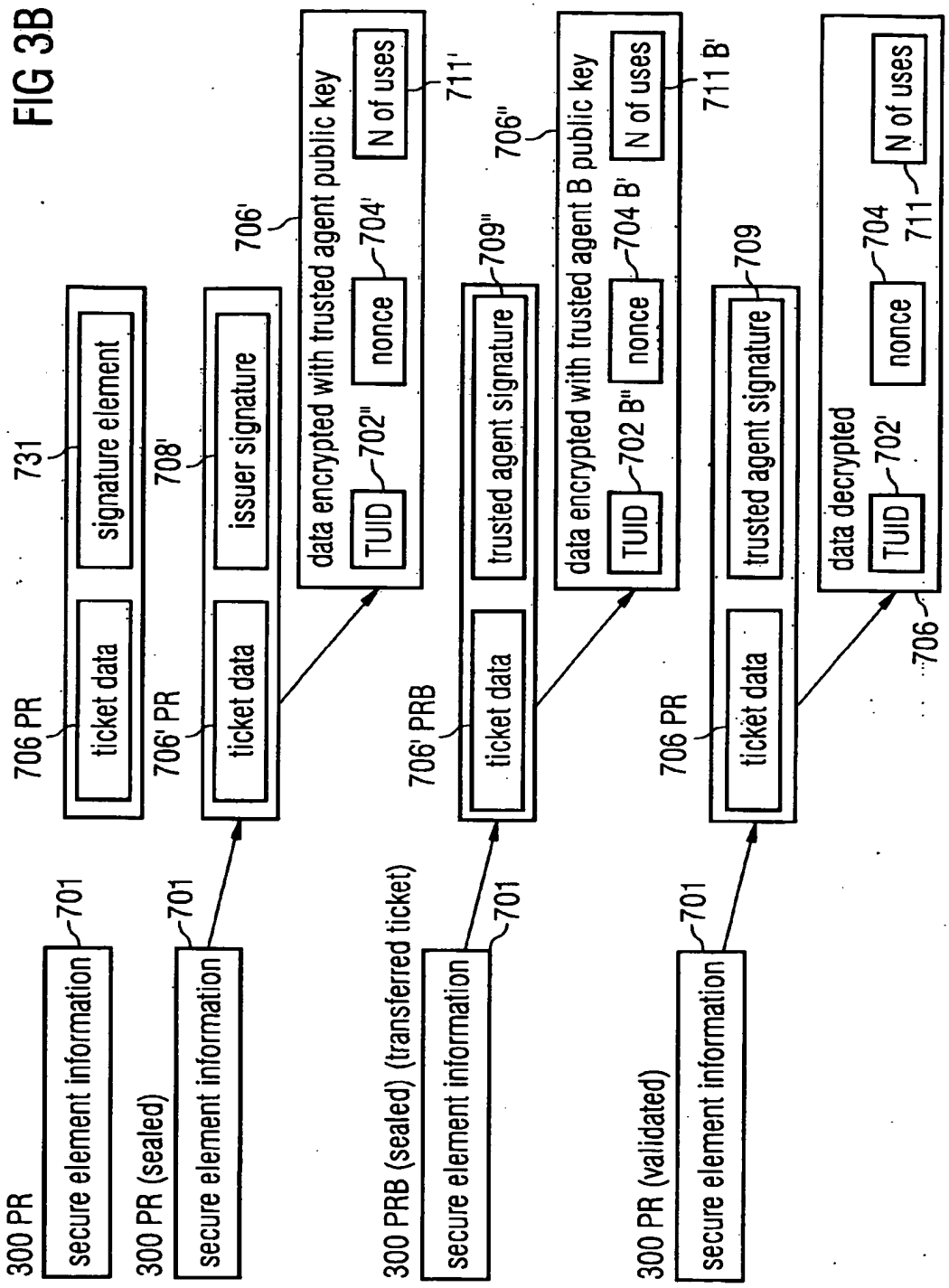

300 PR
secure element information
701
706 PR
ticket data
731
signature element
300 PR (sealed)
secure element information
701
706' PR
ticket data
708'
issuer signature
706'
data encrypted with trusted agent public key
TUID
702"
nonce
704'
N of uses
711'
300 PRB (sealed) (transferred ticket)
secure element information
701
706' PRB
ticket data
709"
trusted agent signature
706"
data encrypted with trusted agent B public key
TUID
702 B"
nonce
704 B'
N of uses
711 B'
300 PR (validated)
secure element information
701
706 PR
ticket data
709
trusted agent signature
data decrypted
TUID
702'
nonce
704
711
N of uses
706

FIG 3C

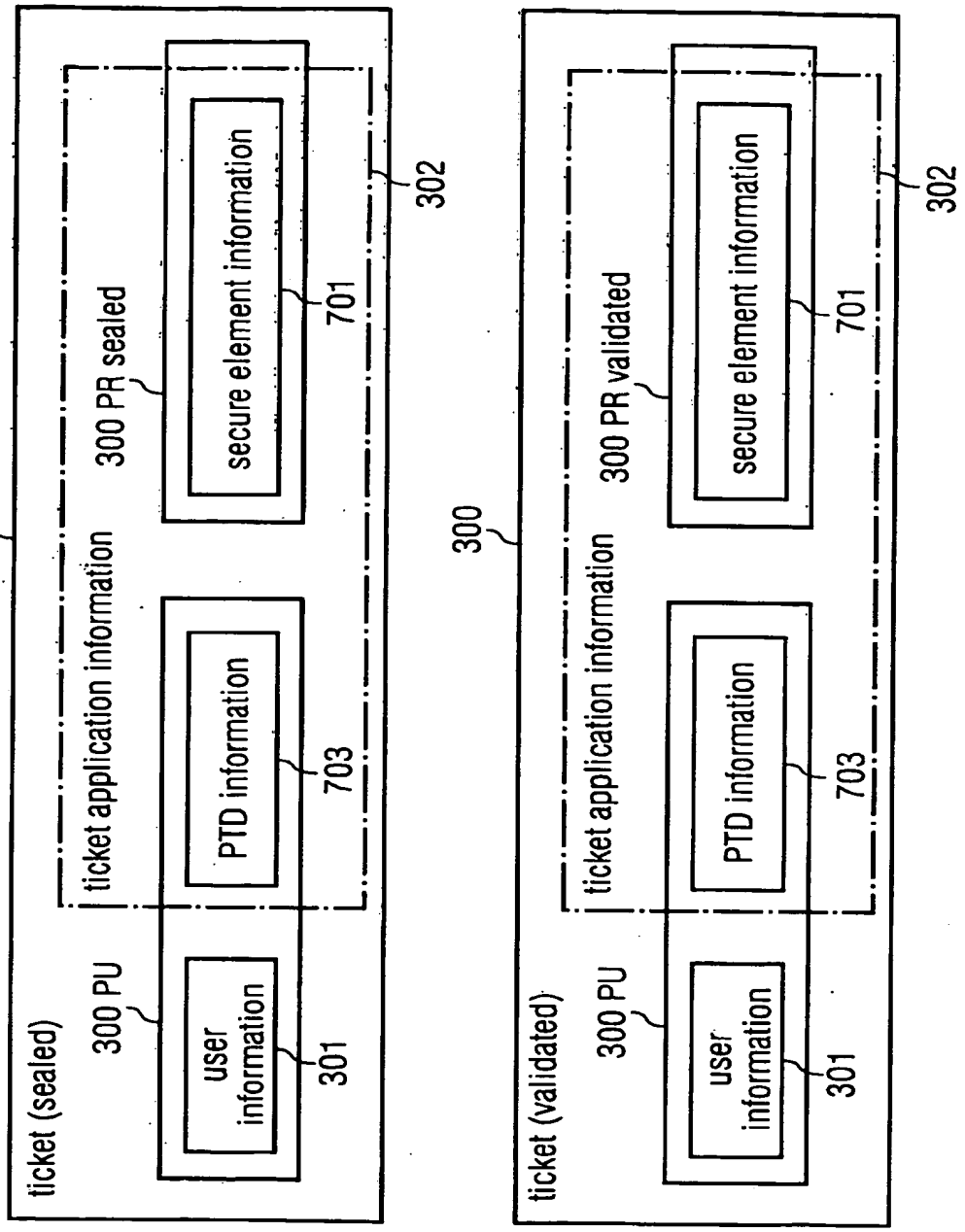

ticket (sealed)
300
ticket application information
300 PU
user information
301
PTD information
703
300 PR sealed
secure element information
701
302
ticket (validated)
300
ticket application information
300 PU
user information
301
PTD information
703
300 PR validated
secure element information
701
302

FIG 4

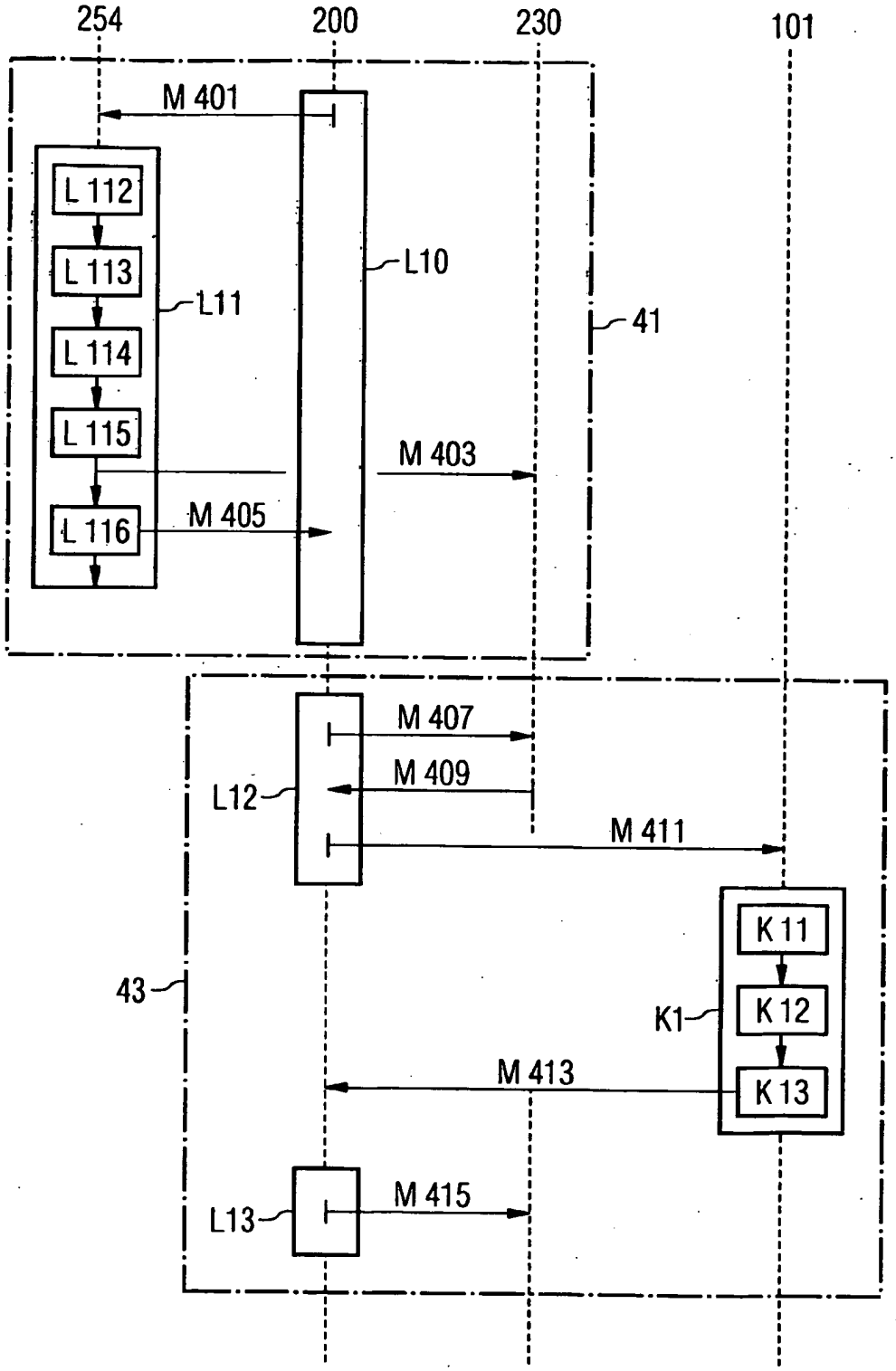

254
200
230
101
M 401
L 112
L 113
L 114
L 115
L 116
L11
L10
41
M 403
M 405
M 407
M 409
L12
M 411
K 11
K 12
K 13
K1
43
M 413
M 415
L13

FIG 5

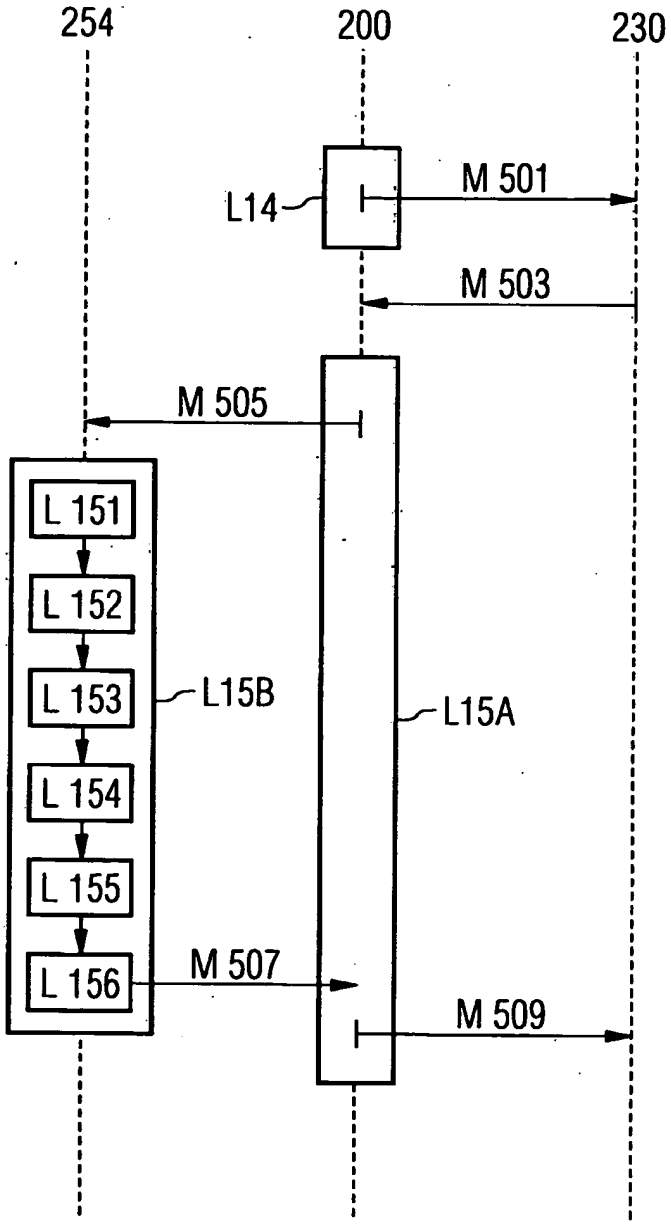

254
200
230
L14
M 501
M 503
M 505
L 151
L 152
L 153
L 154
L 155
L 156
L15B
L15A
M 507
M 509

FIG 6A

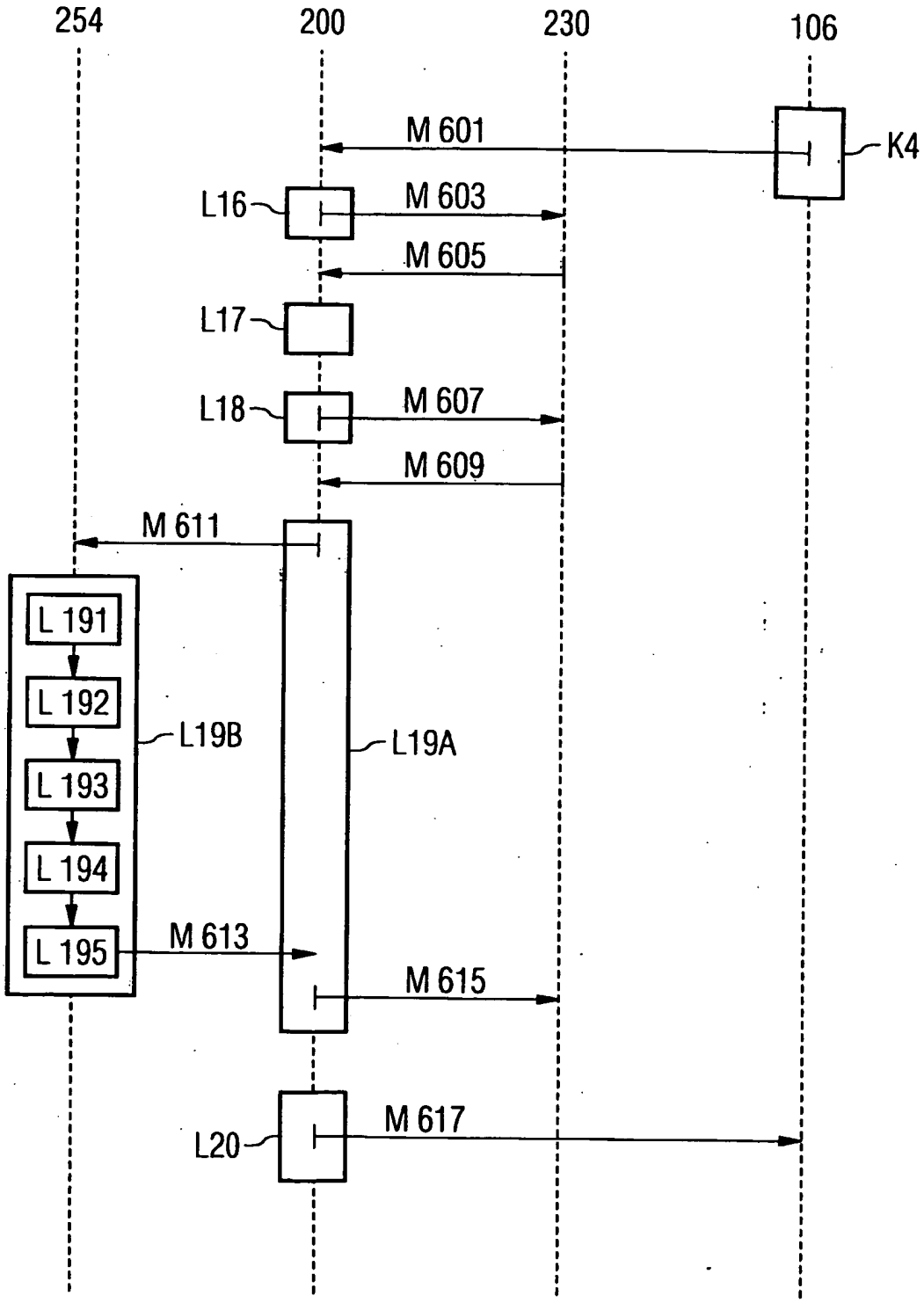

254
200
230
106
M 601
K4
L16
M 603
M 605
L17
L18
M 607
M 609
M 611
L 191
L 192
L 193
L 194
L 195
L19B
L19A
M 613
M 615
L20
M 617

FIG 6B

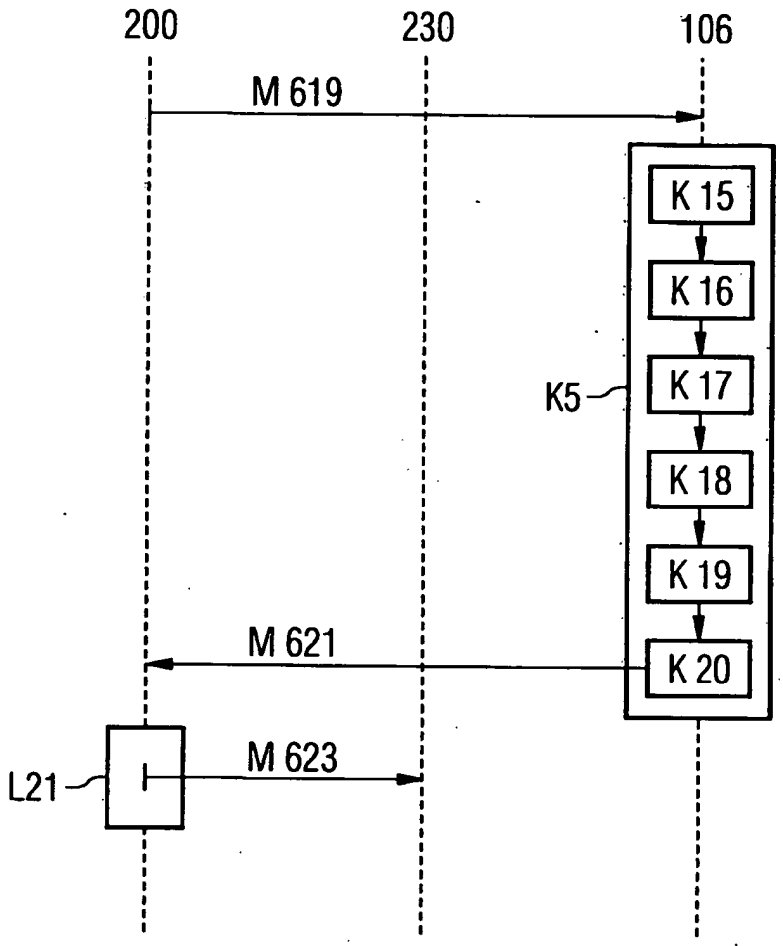
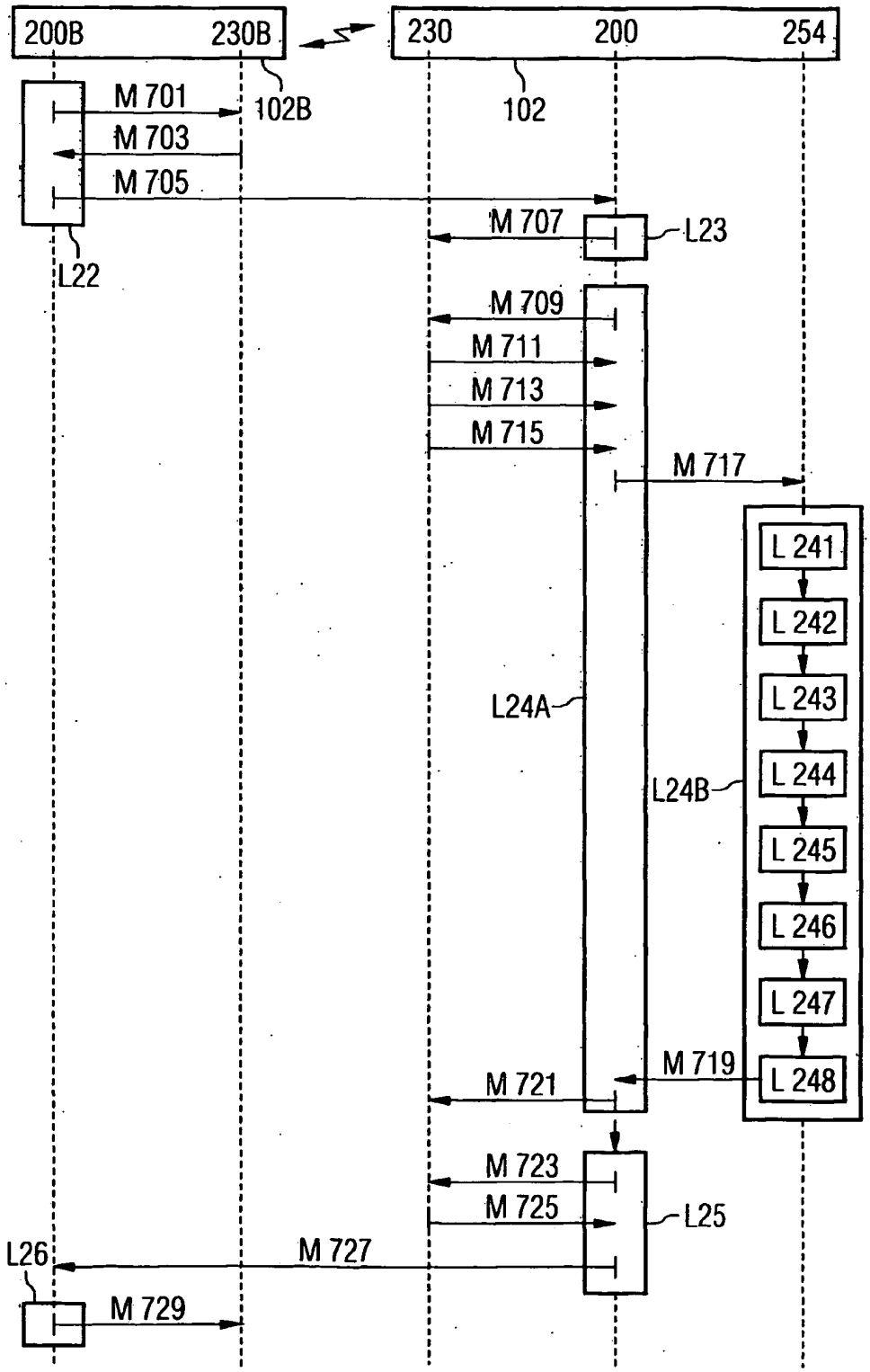


FIG 7


200B
230B
230
200
254
102B
102
M 701
M 703
M 705
M 707
L23
L22
M 709
M 711
M 713
M 715
M 717
L 241
L 242
L 243
L 244
L 245
L 246
L 247
L 248
L24A
L24B
M 719
M 721
M 723
M 725
L25
L26
M 727
M 729

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 00 1026

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	EP 0 980 052 A (NIPPON TELEGRAPH & TELEPHONE) 16 February 2000 (2000-02-16) * paragraph '0020! - paragraph '0042! * * paragraph '0064! - paragraph '0075! * * figures 1-3,14-16 *	1-27	G07B15/00 G07C9/00
X	GB 2 317 790 A (BILLINGSLEY RICHARD) 1 April 1998 (1998-04-01) * page 4, line 23 - page 12, line 32 * * claims; figures *	1-3, 12-16,18	
X	EP 0 823 694 A (NEDERLAND PTT) 11 February 1998 (1998-02-11)	15,27	
A	* figures * * column 3, line 34 - column 5, line 19 *	1,16	
A	EP 1 150 228 A (FOURNIR LTD) 31 October 2001 (2001-10-31) * abstract; claims; figures *	1-27	
A	US 6 493 550 B1 (RAITH ALEX KRISTER) 10 December 2002 (2002-12-10) * column 3, line 5 - line 50 * * figures *	14,17, 19-24	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G07B G07C G07F
A	US 5 569 897 A (MASUDA HIDEHIRO) 29 October 1996 (1996-10-29)		
A	EP 1 065 637 A (HITACHI LTD) 3 January 2001 (2001-01-03)		

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	29 July 2003	Miltgen, E

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 00 1026

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

29-07-2003

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
EP 0980052	A	16-02-2000	CA	2280269 C	29-04-2003
			EP	0980052 A2	16-02-2000
			JP	2000123095 A	28-04-2000
GB 2317790	A	01-04-1998	AU	4216597 A	17-04-1998
			WO	9813795 A1	02-04-1998
EP 0823694	A	11-02-1998	EP	0823694 A1	11-02-1998
			AT	213558 T	15-03-2002
			AU	718123 B2	06-04-2000
			AU	4118097 A	06-03-1998
			CA	2262760 C	05-11-2002
			DE	69710588 D1	28-03-2002
			DE	69710588 T2	05-09-2002
			WO	9807120 A1	19-02-1998
			EP	0920681 A1	09-06-1999
			ES	2172809 T3	01-10-2002
			NZ	334055 A	23-02-2001
			US	6119945 A	19-09-2000
EP 1150228	A	31-10-2001	EP	1150228 A1	31-10-2001
US 6493550	B1	10-12-2002	AT	226005 T	15-10-2002
			AU	759235 B2	10-04-2003
			AU	1718300 A	13-06-2000
			CN	1326661 T	12-12-2001
			DE	69903467 D1	14-11-2002
			DE	69903467 T2	26-06-2003
			EP	1131975 A1	12-09-2001
			ES	2185410 T3	16-04-2003
			JP	2002531031 T	17-09-2002
			WO	0032002 A1	02-06-2000
US 5569897	A	29-10-1996	JP	2783971 B2	06-08-1998
			JP	7210730 A	11-08-1995
EP 1065637	A	03-01-2001	JP	2001014409 A	19-01-2001
			EP	1065637 A2	03-01-2001

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82